Acronis® Backup and Security 2010

Manuale dell'utente

Acronis Backup and Security 2010
Manuale dell'utente

Pubblicato 2010.04.19

Avvertimenti Legali

Indice

Prefazione

Questa Guida è destinata a tutti gli utenti che hanno scelto **Acronis Backup and Security 2010** come soluzione di sicurezza per i loro personal computers. L'informazione presentata in questo manuale è indicata non solo a esperti di computers, ma è accessibile a tutti quelli in grado di lavorare con Windows.

Questo manuale illustra Acronis Backup and Security 2010, e il processo di installazione e configurazione. Sarà possibile imparare ad utilizzare Acronis Backup and Security 2010, ad aggiornarlo, testarlo e personalizzarlo, in pratica come sfruttare al meglio Acronis Backup and Security 2010.

Ti auguriamo una lettura gradevole e utile.

1. Convenzioni usate in questo manuale

1.1. Convenzioni tipografiche

Nel libro vengono usati diversi stili di testo per una leggibilità migliorata. Il loro aspetto e significato vengono presentati nella tabella sottostante.

Aspetto	Descrizione
`sample syntax`	Gli esempi sintattici vengono scritte con caratteri `monospazio`.
http://www.acronis.it/support/	I link URL puntano su alcuna ubicazione esterna, su server http o ftp.
«Prefazione» (p. ix)	Questo è un link interno, verso qualche ubicazione nel documento.
`filename`	File e directory (cartelle) vengono scritte con fonti `monospazio`.
option	Tutte le opzioni del prodotto vengono scritte usando caratteri in **grassetto**.

1.2. Avvertenze

Le avvertenze appaiono in note di testo, segnalate graficamente, offrendo alla tua attenzione informazione addizionale relativa al paragrafo corrente.

Nota

La nota è solo una piccola osservazione. Anche se la puoi omettere, la nota può provvedere informazione di valore come una caratteristica specifica o un link verso temi relazionati.

Importante

Questa richiede la tua attenzione e non è consigliato saltarla. Solitamente facilita informazione non critica ma significante.

Avvertimento

Questa è un’informazione critica che dovresti trattare con crescente cautela. Niente di male accadrà se segui le istruzioni. Dovresti leggerlo e capirlo, perché descrive qualcosa di estremamente rischioso.

2. Struttura del manuale

Il manuale è composto da diverse parti contenenti gli argomenti importanti. Inoltre, viene anche fornito un glossario per chiarire alcuni termini tecnici.

Installazione e rimozione. Istruzioni passo passo per l'installazione di Acronis Backup and Security 2010 su un personal computer. Partendo dai prerequisiti per una installazione valida, l'utente viene guidato lungo l'intero processo di installazione. Infine la procedura di rimozione viene descritta nel caso si abbia bisogno di disinstallare Acronis Backup and Security 2010.

Iniziando. Contiene tutte le informazioni necessarie a muovere i primi passi con Acronis Backup and Security 2010. Viene presentata l'interfaccia di Acronis Backup and Security 2010 e le procedure per risolvere i problemi, configurare le impostazioni di base e registrare il prodotto.

Modalità intermedia. Presenta l'interfaccia Modalità Intermedia di Acronis Backup and Security 2010.

Modalità avanzata. Una descrizione dettagliata dell'interfaccia Modalità Avanzata di Acronis Backup and Security 2010. Vi spieghiamo come configurare ed utilizzare tutti i moduli di Acronis Backup and Security 2010 in modo da proteggere efficacemente il vostro computer da ogni tipo di minaccia (malware, spam, hackers, contenuto inappropriato ed altro).

Integrazione in Software Windows e di terzi . Mostra come utilizzare le opzioni di Acronis Backup and Security 2010 dal menu contestuale di Windows e dalla barra degli strumenti Acronis integrata in programmi supportati di terze parti.

Come fare. Procedura per le funzioni più comuni in Acronis Backup and Security 2010

Risoluzione dei problemi e aiuto. Dove cercare e ottenere un aiuto in caso di difficoltà.

Glossario. Il glossario cerca di spiegare alcuni termini tecnici e poco comuni che troverai tra le pagine di questo documento.

Installazione e rimozione

1. Requisiti del sistema

È possibile installare Acronis Backup and Security 2010 solo su computer con i seguenti sistemi operativi:

- Windows XP (32/64 bit) con Service Pack 2 o superiore
- Windows Vista (32/64 bit) o Windows Vista con Service Pack 1 o successivo
- Windows 7 (32/64 bit)

Prima dell'installazione, assicurarsi che il computer soddisfa i prerequisiti hardware e software minimi.

Nota
Per verificare il sistema operativo sul computer e l'informazione hardware, fare clic con il pulsante destro del mouse su **Risorse del computer** sul desktop e quindi selezionare **Proprietà** dal menu.

1.1. Requisiti minimi di sistema

- 450 MB di spazio disponibile su disco rigido
- Processore da 800 MHz
- RAM:
  - 512 MB per Windows XP
  - 1 GB per Windows Vista/Windows 7
- Internet Explorer 6.0
- .NET Framework 1.1 (disponibile anche nel kit d'installazione)

1.2. Requisiti di sistema consigliati

- 600 MB di spazio disponibile su disco rigido
- Intel CORE Duo (1.66 GHz) o processore equivalente
- RAM:
  - 1 GB per Windows Vista/Windows 7
  - 1,5 GB per Windows Vista
- Internet Explorer 7 (o superiore)
- .NET Framework 1.1 (disponibile anche nel kit d'installazione)

1.3. Software supportato

La protezione antiphishing viene fornita solo per:

- Internet Explorer 6.0 o superiore
- Mozilla Firefox 2.5 o superiore
- Yahoo Messenger 8.5 o superiore
- Windows Live Messenger 8 o superiore

La criptazione del Chat (IM) viene fornita solo per:

- Yahoo Messenger 8.5 o superiore
- Windows Live Messenger 8 o superiore

È fornita una protezione antispam per tutti i client di posta POP3/SMTP. La barra degli strumenti di Acronis Backup and Security 2010 Antispam è integrata solo in:

- Microsoft Outlook 2000 / 2003 / 2007
- Microsoft Outlook Express
- Microsoft Windows Mail
- Thunderbird 2.0.0.17

2. Preparazione all'Installazione

Prima di installare Acronis Backup and Security 2010, completare questi passi preliminari per assicurarsi che l'installazione funzioni senza problemi:

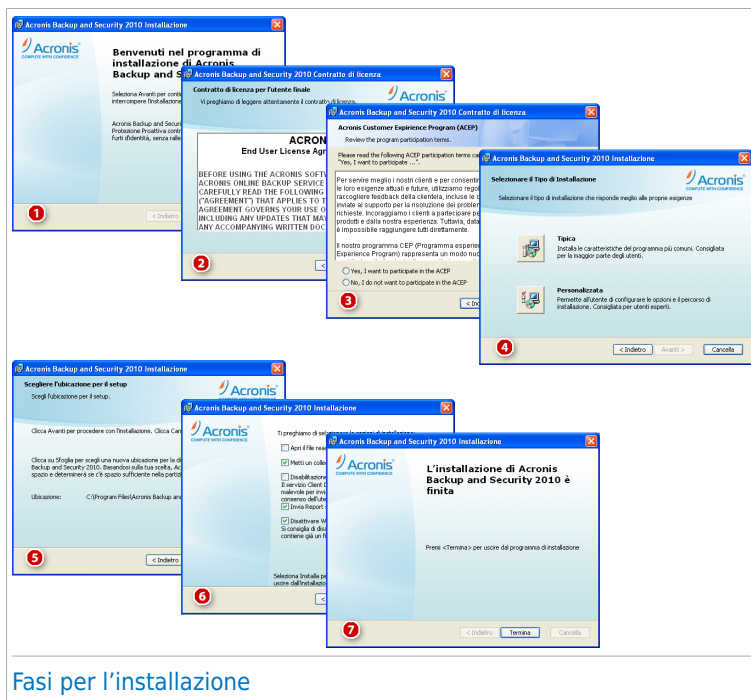
- Assicurarsi che il computer su cui si desidera installare Acronis Backup and Security 2010 risponda ai requisiti minimi di sistema. Se il computer non risponde ai requisiti minimi di sistema, Acronis Backup and Security 2010 non verrà installato o se installato non funzionerà correttamente e causerà rallentamenti e instabilità del sistema. Per un elenco completo dei requisiti di sistema, fare riferimento a *«Requisiti del sistema»* (p. 2).
- Accedere al computer utilizzando un account Amministratore.
- Rimuovere qualsiasi altro software di sicurezza dal computer. L'esecuzione simultanea di due programmi di sicurezza può influenzarne il funzionamento e causare problemi seri al sistema. Windows Defender sarà disabilitato per default prima dell'avvio dell'installazione.
- Disabilitare o rimuovere qualsiasi programma firewall che possa essere in esecuzione sul computer. L'esecuzione simultanea di due programmi firewall può influenzarne il funzionamento e causare problemi seri al sistema. Windows Firewall sarà disabilitato per default prima dell'avvio dell'installazione.

3. Installazione di Acronis Backup and Security 2010

Può acquistare e scaricare il file di installazione dal sito Acronis Inc.:

http://www.acronis.it/homecomputing/

Per installare Acronis Backup and Security 2010, salvi il file di installazione sul proprio computer e faccia doppio click. Questo lancerà una procedura guidata, che la guiderà attraverso il processo di installazione.

Il programma di installazione controllerà innanzitutto il sistema per convalidare l'installazione. Se l'installazione viene convalidata, apparirà l'assistente di setup. L'immagine seguente illustra i passaggi dell'assistente di setup.

Fasi per l'installazione

Seguire questi passi per installare Acronis Backup and Security 2010:

1. Selezionare **Avanti**. E' possibile annullare l'installazione in qualsiasi momento facendo clic su **Annulla**.

   Acronis Backup and Security 2010 avvisa se vi sono altri prodotti antivirus installati sul computer. Selezionare **Rimuovi** per disinstallare il corrispondente prodotto. Se si desidera continuare senza rimuovere i prodotti rilevati, selezionare **Avanti**.

Avvertimento

Si raccomanda di disinstallare qualsiasi altro prodotto antivirus precedentemente installato. Infatti due o più antivirus sulla stessa macchina potrebbero rendere il sistema inutilizzabile.

2. Vi preghiamo di leggere il Contratto di Licenza, e selezionare **Accetto**

Importante

Se non siete d'accordo con le condizioni del contratto, selezionare **Cancella**. Il processo di installazione verrà abbandonato ed uscirete dal setup.

3. Al fine di fornire prodotti migliori, Acronis ha creato un Programma di attenzione al Cliente (Customer Experience Program). La preghiamo di leggere attentamente i termini del programma e selezionare se vuole partecipare al programma.

   Selezionare **Successivo** per continuare.

4. Selezionare il tipo di installazione da eseguire.
   - **Tipica** - per installare il programma immediatamente, utilizzando le opzioni di installazione di default. Se si seleziona questa opzione, passare al Passo 6.
   - **Personalizzata** - per configurare le opzioni di installazione e quindi installare il programma. Questa opzione permette di modificare il percorso di installazione.

5. Per default, Acronis Backup and Security 2010 verrà installato in `C:\Program Files\Acronis Backup and Security\Acronis Backup and Security 2010`. Se si desidera modificare il percorso d'installazione, fare clic su **Sfoglia**, quindi selezionare, la cartella dove si desidera installare Acronis Backup and Security 2010.

   Selezionare **Avanti**.

6. Selezionare le opzioni relative al processo di installazione. Le opzioni consigliate sono selezionate per default:
   - **Apri il file readme** - per aprire il file leggimi al termine dell'installazione.
   - **Metti un collegamento sul desktop** - per mettere un collegamento a Acronis Backup and Security 2010 sul desktop al termine dell'installazione.
   - **Disabilita Caching DNS** - per disabilitare il Caching DNS (Domain Name System). Il servizio Client DNS può essere utilizzato da applicazioni malevole per inviare informazioni attraverso la rete senza il consenso dell'utente.
   - **Invia Rapporti Virus** - per inviare rapporti sulla scansione antivirus al Laboratorio Acronis per l'analisi. I report non conterranno dati confidenziali, come il vostro nome o indirizzo IP, e non verranno utilizzati per scopi commerciali.
   - **Disattiva il Firewall di Windows** - per disattivare il Firewall di Windows.

Importante

Si raccomanda di disabilitare il Firewall di Windows poiché Acronis Backup and Security 2010 include già un firewall avanzato. Far funzionare due firewall sullo stesso computer può causare dei problemi.

- **Disattiva Windows Defender** - per disattivare Windows Defender; questa opzione compare slo su Windows Vista.

Fare clic su **Installa** per avviare l'installazione. Se non è stato ancora installato, Acronis Backup and Security 2010 installerà per prima .NET Framework 1.1.

4. Attivazione del prodotto

Dopo il riavvio successivo all'installazione, il programma funzionerà in modalità di prova per 30 giorni. Durante questo periodo il prodotto deve essere attivato. Diversamente, smetterà di funzionare.

All'acquisto del prodotto, si riceve un numero di serie di 16 caratteri, nella confezione o per posta elettronica. Il numero di serie di 64 caratteri richiesto per l'attivazione del prodotto verrà inviato all'indirizzo di posta elettronica dell'utente dopo che avrà immesso il numero di serie di 16 caratteri nella pagina Web di registrazione.

L'abbonamento annuale al prodotto decorre a partire dal momento in cui viene inviato il numero di serie di 64 caratteri. Al termine del periodo di abbonamento, la licenza scadrà e non sarà possibile utilizzare il prodotto. Per sbloccare il prodotto, sarà necessario acquistare una nuova licenza. L'utente riceverà per posta elettronica un nuovo numero di serie di 16 caratteri e dovrà eseguire di nuovo la procedura di attivazione.

Procedura dettagliata di attivazione

Quando il programma viene avviato per la prima volta, all'utente viene chiesto se dispone del numero di serie di 64 caratteri.

Caso 1: l'utente dispone del numero di serie di 64 caratteri.

1. Fare clic su **Sì**.
2. Nella pagina successiva, incollare il numero di serie nella casella appropriata (tramite la combinazione di tasti CTRL+V).
3. Fare clic sul pulsante **Attiva**.

Caso 2: l'utente non dispone del numero di serie di 64 caratteri, ma di quello di 16 caratteri.

1. Fare clic sul pulsante **Numero di serie**.
2. Sul sito Web, immettere le informazioni sul proprio account Acronis, il numero di serie di 16 caratteri e il proprio l'indirizzo di posta elettronica. All'indirizzo di posta elettronica specificato verrà inviato un messaggio con il numero di serie di 64 caratteri.

   Se non si possiede ancora un account Acronis, questo verrà creato utilizzando le informazioni personali specificate al momento della registrazione del prodotto.
3. Aprire il messaggio di posta elettronica ricevuto e copiare il numero di serie.
4. Tornare al programma e fare clic sul pulsante **Sì**.
5. Nella pagina successiva, incollare il numero di serie nella casella appropriata (tramite la combinazione di tasti CTRL+V).

6. Fare clic sul pulsante **Attiva**.

Caso 3: l'utente non possiede né il numero di serie di 16 caratteri, né quello di 64 caratteri.

1. Fare clic sul collegamento **Acquista online**.
2. Acquistare il prodotto. Il numero di serie di 16 caratteri verrà inviato all'indirizzo di posta elettronica dell'utente.
3. Eseguire tutti i passaggi del caso 2.

Caso 4: l'utente non dispone di nessun numero di serie e desidera prima provare il prodotto.

1. Fare clic sul pulsante **In seguito**. L'utente avrà a disposizione il prodotto completamente funzionante per il periodo di prova.
2. Se si decide di acquistare il prodotto, eseguire tutti i passaggi del caso 3.

5. Riparare o Rimuovere Acronis Backup and Security 2010

Se si desidera riparare o rimuovere Acronis Backup and Security 2010, seguire questo percorso dal menu di avvio di Windows: **Start** → **Programmi** → **Acronis** → **Acronis Backup and Security 2010** → **Ripara o Rimuovi**.

Vi verrà richiesto di confermare la vostra scelta selezionando **Avanti**. Apparirà una nuova finestra dove potrete selezionare:

- **Riparare** - per re-installare tutte le componenti del programma installate dal setup precedente.

  Scegliendo di riparare Acronis Backup and Security 2010, la seguente nuova finestra comparirà. Selezionare **Riparare** per iniziare il processo di riparazione.

  Riavviare il computer quando venga richiesto, e quindi selezionare **Installa** per reinstallare Acronis Backup and Security 2010.

  Una volta completato il processo di installazione, apparirà una nuova finestra. Selezionare **Termina**.

- **Rimuovi** - per rimuovere tutte le componenti installate.

Nota

Vi consigliamo di scegliere **Rimuovere** per una reinstallazione pulita.

Scegliendo di rimuovere Acronis Backup and Security 2010, apparirà una nuova finestra.

Importante

Rimuovendo Acronis Backup and Security 2010, non sarete più protetti da virus, spyware e hacker. Se desiderate che Windows Firewall e Windows Defender (solo su Windows Vista) vengano attivati dopo aver disinstallato Acronis Backup and Security 2010, selezionare le caselle corrispondenti.

Selezionare **Rimuovere** per iniziare la rimozione di Acronis Backup and Security 2010 dal vostro computer.

Una volta completato il processo di rimozione, apparirà una nuova finestra. Selezionare **Termina**.

Nota

Al termine del processo di disinstallazione, consigliamo di cancellare la cartella `Acronis Backup and Security` dei `Program Files`.

Iniziando

6. Panoramica

Una volta che avrete installato Acronis Backup and Security 2010 il vostro computer sarà protetto.

6.1. Apertura di Acronis Backup and Security 2010

Per accedere all'interfaccia principale di Acronis Backup and Security 2010, usare il menu Start di Windows, seguendo il percorso: **Start** → **Programmi** → **Acronis** → **Acronis Backup and Security 2010** → **Acronis Backup and Security 2010** o più rapidamente facendo doppio clic sull'icona Acronis presente nella barra delle applicazioni.

6.2. Modalità di visualizzazione dell'interfaccia dell'utente.

Acronis Backup and Security 2010 soddisfa le necessità di persone esperte e di principianti. L'interfaccia grafica dell'utente è quindi stata progettata per essere adatta a qualsiasi categoria di utenti.

È possibile selezionare visualizzazione l'interfaccia utente in base a tre diverse modalità, a seconda della propria conoscenza dei computer e di Acronis.

Modalità	Descrizione
Modalità inesperto	Adatta per principianti e per persone che desiderano che Acronis Backup and Security 2010 protegga il proprio computer e i dati senza essere tanti problemi. Questa modalità è di facile utilizzo e richiede un intervento minimo da parte dell'utente. La sola cosa da fare è risolvere i problemi indicati da Acronis Backup and Security 2010. Una facile procedura guidata aiuterà a risolvere i problemi. Inoltre è possibile compiere attività comuni quale l'aggiornamento delle firme dei virus di Acronis Backup and Security 2010 e dei file del prodotto, oppure la scansione del computer.
Modalità intermedia	Rivolta ad utenti con una conoscenza media di computer, questa modalità amplia le funzionalità presenti nella Modalità inesperto. È possibile risolvere problemi separatamente e scegliere quali problemi monitorare. Inoltre è possibile gestire in remoto prodotti Acronis installati su computer della propria casa.

Modalità	Descrizione
Modalità avanzata	Adatta ad utenti esperti, questa modalità consente di configurare ogni funzionalità di Acronis Backup and Security 2010. Inoltre è possibile utilizzare tutte le attività fornite per proteggere il proprio computer e i dati.

Di default, l'interfaccia utente viene mostrata nella Modalità Intermedia. Per cambiare modalità di interfaccia utente, eseguire i seguenti passi:

1. Apri Acronis Backup and Security 2010.
2. Fare clic sul pulsante **Impostazioni** in alto a destra.
3. Nella categoria Impostazioni interfaccia utente, fare clic sulla freccia sul pulsante e selezionare la modalità desiderata dal menu.
4. Fare clic su **OK** per salvare e applicare i cambiamenti.

6.2.1. Modalità inesperto

Se si è inesperti in materia di computer, l'interfaccia Modalità inesperto potrebbe essere la scelta migliore. Questa modalità è semplice da utilizzare e richiede pochissimo intervento da parte dell'utente.

Modalità inesperto

La finestra è suddivisa in quattro sezioni principali:

- **Stato della sicurezza** informa in merito ai problemi che riguardano la sicurezza del computer e aiuta a risolverli. Facendo clic su **Risolvi tutto**, una procedura guidata aiuterà a risolvere facilmente minacce alla sicurezza del computer e dei dati. Per ulteriori informazioni, far riferimento a *«Risolvi i Problemi»* (p. 34).
- In **Proteggi il PC** è possibile trovare le attività che proteggono il computer e i dati. Le attività disponibili che possono essere eseguite sono diverse a seconda del profilo di utilizzo selezionato.
  - Il pulsante **Esegui scansione Ora** avvia una scansione standard del sistema alla ricerca di virus, spyware e altro malware. Appare la procedura guidata Antivirus Scan che illustra il processo di scansione. Per ulteriori informazioni sulla procedura guidata, far riferimento a *«Procedura guidata scansione antivirus»* (p. 46).
  - Il pulsante **Aggiorna Ora** permette di aggiornare le firme dei virus e i file di prodotto di Acronis Backup and Security 2010. Apparirà una nuova finestra, dove potrete visualizzare lo stato dell'aggiornamento. Se vengono rilevati degli aggiornamenti, questi vengono automaticamente scaricati ed installati sul computer.
  - Quando viene selezionato il profilo **Tipico** il pulsante **Controllo Vulnerabilità** esegue un assistente che permette di trovare e risolvere le vulnerabilità del sistema, quali ad esempio del software obsoleto o degli aggiornamenti di Windows mancanti. Per ulteriori informazioni fare riferimento alla sezione *«Procedura guidata di Controllo delle vulnerabilità»* (p. 58).
  - Quando viene selezionato il profilo **Giocatore** il pulsante **Attiva/disattiva Modalità Gioco** permette di attivare/disattivare la Modalità Gioco. La Modalità Gioco modifica temporaneamente le impostazioni di protezione in modo di minimizzare l'impatto sulle prestazioni del sistema.
- In **Manutenzione del PC** è possibile trovare le attività aggiuntive che proteggono il computer e i dati.
  - **Aggiungi File al Vault** - inizia la procedura guidata che permette di immagazzinare i file / documenti importanti privatamente mediante la criptazione in speciali drive protetti.
  - **Scansione Approfondita del Sistema** avvia una scansione completa del sistema alla ricerca di tutti i tipi di malware.
  - **Scansione Documenti** effettua la scansione alla ricerca di virus e altro malware nelle cartelle utilizzate più comunemente: `Documenti` e `Desktop`. Questo assicura la sicurezza dei documenti, un'area di lavoro sicura e l'esecuzione di applicazioni pulite all'avvio.
- **Profili D'uso** indica il profilo di utilizzo correntemente selezionato. Il profilo di utilizzo rispecchia le attività principali eseguite sul computer. A seconda del profilo

di utilizzo, l'interfaccia del prodotto è organizzata in modo da permettere facile accesso alle attività preferite.

Se si desidera passare ad un profilo differente oppure modificare il profilo attualmente in uso, fare clic sul profilo e seguire l'assistente di configurazione.

Nell'angolo in alto a destra della finestra è possibile vedere il pulsante **Impostazioni**. Apre una finestra in cui è possibile cambiare la modalità dell'interfaccia utente e abilitare o disabilitare le impostazioni principali di Acronis Backup and Security 2010. Per ulteriori informazioni, ti preghiamo di far riferimento a *«Configurazione delle Impostazioni di base»* (p. 38).

Nell'angolo in basso a destra della finestra è possibile trovare diversi link utili.

Link	Descrizione
Compra/Rinnova	Apre una pagina web dove è possibile acquistare una chiave di licenza per il prodotto Acronis Backup and Security 2010.
Supporto	Vi permette di contattare il team di supporto di Acronis
Aiuto	Ti da accesso ad un file di aiuto che ti insegna ad usare Acronis Backup and Security 2010.
Registri	Vi permette di visualizzare una cronologia dettagliata di tutti i task eseguiti da Acronis Backup and Security 2010 nel vostro sistema.

6.2.2. Modalità intermedia

Ricolta agli utenti con una conoscenza media dei computer, la Modalità Intermedia è una interfaccia semplice che fornisce accesso a tutti i moduli di base. Si dovranno monitorare avvertimenti e avvisi critici e risolvere problemi.

Modalità intermedia

La finestra Modalità Intermedia contiene 5 schede. La seguente tabella descrive brevemente ogni scheda. Per ulteriori informazioni, far riferimento alla parte «Modalità intermedia» (p. 84) di questo manuale.

Tab	Descrizione
Dashboard	Visualizza lo stato di sicurezza del sistema e permette di ripristinare il profilo di utilizzo.
Sicurezza	Mostra lo stato dei moduli di sicurezza (antivirus, antiphishing, firewall, antispam, criptazione chat, privacy, controllo vulnerabilità e moduli di aggiornamento) insieme ai links per le funzioni antivirus, aggiornamento e controllo vulnerabilità.
Genitori	Mostra lo stato del modulo Controllo genitori. Il Controllo genitori consente di restringere l'accesso a Internet e a applicazioni specifiche da parte dei figli.
File Vault	Mostra lo stato della criptazione dei file insieme ai link per accedervi.
Rete	Mostra la struttura della rete domestica Acronis. Qui puoi attivare varie azioni per configurare e cgestire i prodotti Acronis installati sulla tua rete casalinga In questo modo puoi gestire la sicurezza della tua rete di casa da una singola postazione

Nell'angolo in alto a destra della finestra è possibile vedere il pulsante **Impostazioni**. Apre una finestra in cui è possibile cambiare la modalità dell'interfaccia utente e abilitare o disabilitare le impostazioni principali di Acronis Backup and Security 2010. Per ulteriori informazioni, ti preghiamo di far riferimento a *«Configurazione delle Impostazioni di base»* (p. 38).

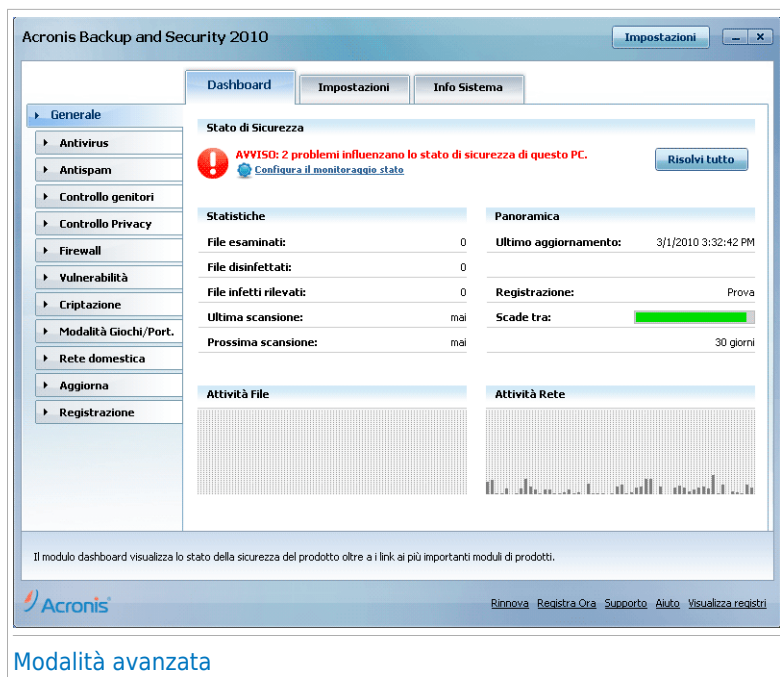
Nell'angolo in basso a destra della finestra è possibile trovare diversi link utili.

Link	Descrizione
Compra/Rinnova	Apre una pagina web dove è possibile acquistare una chiave di licenza per il prodotto Acronis Backup and Security 2010.
Registrare	Vi permette di inserire il numero di serie e vedere lo stato della registrazione.
Supporto	Vi permette di contattare il team di supporto di Acronis
Aiuto	Ti da accesso ad un file di aiuto che ti insegna ad usare Acronis Backup and Security 2010.
Registri	Vi permette di visualizzare una cronologia dettagliata di tutti i task eseguiti da Acronis Backup and Security 2010 nel vostro sistema.

6.2.3. Modalità avanzata

La Modalità Avanzata dà accesso ad ogni specifico componente di Acronis Backup and Security 2010. Qui è possibile configurare in dettaglio Acronis Backup and Security 2010.

Nota

La Modalità Avanzata è adatta per utenti dotati di conoscenze informatiche superiori alla media, che conoscono a quali tipi di pericoli è esposto un computer e come funzionano i programmi di sicurezza.

Modalità avanzata

Sulla parte sinistra della finestra c'è un menu contenente tutti i moduli di sicurezza. Ogni modulo consiste di una o più schede che permettono la configurazione delle impostazioni di sicurezza corrispondenti oppure permettono di eseguire attività di amministrazione e di sicurezza. La seguente tabella descrive brevemente ogni modulo. Per ulteriori informazioni, far riferimento alla parte «Modalità avanzata» (p. 106) di questo manuale.

Modulo	Descrizione
Generale	Vi permette di accedere alle impostazioni generali o di visualizzare la dashboard e le informazioni dettagliate di sistema.
Antivirus	Vi permette di configurare in dettaglio il vostro scudo antivirus e le operazioni di scansione, impostare le eccezioni e configurare il modulo di quarantena.
Antispam	Permette di mantenere la cassetta postale libera da SPAM e di configurare in dettaglio le impostazioni antispam.

Modulo	Descrizione
Controllo dei Genitori	Vi permette di proteggere i vostri bambini dai contenuti inopportuni utilizzando le vostre regole di accesso al computer personalizzate.
Controllo Privacy	Vi permette di prevenire il furto di dati dal vostro computer e proteggere la vostra privacy mentre siete online.
Firewall	Consente di proteggere il computer dai tentativi di connessione non autorizzati sia in entrata che in uscita. È come una guardia al cancello – manterrà sotto controllo la connessione Internet e terrà una registrazione di chi è autorizzato ad accedere ad Internet e chi non lo è.
Vulnerabilità	Vi permette di mantenere aggiornato il software cruciale del vostro computer.
Criptazione	Vi permette di criptare le comunicazioni tramite Yahoo e Windows Live (MSN) Messenger ed anche di criptare localmente i vostri file, cartelle o partizioni critiche.
Modalita' Gioco/Portatile	Vi permette di posporre i task programmati di Acronis mentre il vostro portatile funziona con le batterie ed anche di eliminare allarmi e pop-up mentre giocate.
Rete	Vi permette di configurare e gestire diversi computer nella vostra famiglia.
Aggiornamento	Vi permette di ottenere informazioni sugli ultimi aggiornamenti, di aggiornare il prodotto e di configurare in dettaglio il processo di aggiornamento.

Nell'angolo in alto a destra della finestra è possibile vedere il pulsante **Impostazioni**. Apre una finestra in cui è possibile cambiare la modalità dell'interfaccia utente e abilitare o disabilitare le impostazioni principali di Acronis Backup and Security 2010. Per ulteriori informazioni, ti preghiamo di far riferimento a *«Configurazione delle Impostazioni di base»* (p. 38).

Nell'angolo in basso a destra della finestra è possibile trovare diversi link utili.

Link	Descrizione
Compra/Rinnova	Apre una pagina web dove è possibile acquistare una chiave di licenza per il prodotto Acronis Backup and Security 2010.
Registrare	Vi permette di inserire il numero di serie e vedere lo stato della registrazione.
Supporto	Vi permette di contattare il team di supporto di Acronis

Link	Descrizione
Aiuto	Ti da accesso ad un file di aiuto che ti insegna ad usare Acronis Backup and Security 2010.
Registri	Vi permette di visualizzare una cronologia dettagliata di tutti i task eseguiti da Acronis Backup and Security 2010 nel vostro sistema.

6.3. Configurare Acronis Backup and Security 2010

Acronis Backup and Security 2010 le permette di configurare facilmente le sue impostazioni principali e l'interfaccia, attraverso la creazione di un profilo di utilizzo. Il profilo di utilizzo rispecchia le attività principali eseguite sul computer. A seconda del profilo di utilizzo, l'interfaccia del prodotto è organizzata in modo da permettere facile accesso alle attività preferite.

Di default, il profilo **Tipico** si applica dopo l'installazione di Acronis Backup and Security 2010. Questo profilo è raccomandato principalmente per navigare e per attività multimediali.

Per riconfigurare il profilo di utilizzo, seguire questi passi:

1. Apri Acronis Backup and Security 2010.
2. Fare clic sul pulsante **Impostazioni** in alto a destra.
3. Nella sezione Impostazioni interfaccia utente, clicchi **Reimposta Profilo**.
4. Seguire la procedura guidata di configurazione.

6.3.1. Passo 1 - Selezione del Profilo di Utilizzo

Profili di Utilizzo

Fare clic sul pulsante che descrive al meglio le attività compiute sul computer (il profilo di utilizzo).

Opzione	Descrizione
Tipico	Fare clic qui se il PC è utilizzato principalmente per navigare e per attività multimediali.
Genitore	Fare clic qui se il PC è utilizzato da bambini e si desidera controllarne l'accesso ad Internet utilizzando il modulo Controllo Genitori.
Giocatore	Fare clic qui se il PC è utilizzato principalmente per giocare.
Personalizzato	Fare clic qui se si desiderano configurare tutte le impostazioni principali di Acronis Backup and Security 2010.

Il profilo di utilizzo può essere reimpostato in un secondo momento dall'interfaccia del prodotto.

6.3.2. Passo 2 - Descrivere il Computer

Descrizione del Computer

Selezionare le opzioni che si applicano al computer:

- **Questo computer si trova in una rete domestica.** Selezionare questa opzione se si desidera gestire il prodotto Acronis installato sul computer da remoto (da un altro computer). Un ulteriore passaggio dell'assistente permetterà la configurazione del modulo di Gestione della Rete Domestica.
- **Questo computer è un notebook.** Selezionare questa opzione se si desidera che la Modalità Laptop sia abilitata per default. Nella Modalità portatile, le attività di scansione programmate non vengono eseguite, poiché richiedono più risorse di sistema e, implicitamente, un consumo di energia superiore.

Selezionare **Successivo** per continuare.

6.3.3. Passo 3 - Selezionare l'Interfaccia Utente

Modalità di visualizzazione dell'interfaccia dell'utente.

Fare clic sul pulsante che meglio descrive le capacità informatiche dell'utente per selezionare una modalità di visualizzazione dell'interfaccia utente appropriata. È possibile selezionare visualizzazione l'interfaccia utente in base a tre diverse modalità, a seconda della propria conoscenza dei computer e di Acronis Backup and Security 2010.

Modalità	Descrizione
Modalità inesperto	Adatta per principianti e per persone che desiderano che Acronis Backup and Security 2010 protegga il proprio computer e i dati senza essere tanti problemi. Questa modalità è di facile utilizzo e richiede un intervento minimo da parte dell'utente. La sola cosa da fare è risolvere i problemi indicati da Acronis Backup and Security 2010. Una facile procedura guidata aiuterà a risolvere i problemi. Inoltre è possibile compiere attività comuni quale l'aggiornamento delle firme dei virus di Acronis Backup and Security 2010 e dei file del prodotto, oppure la scansione del computer.

Modalità	Descrizione
Modalità intermedia	Rivolta ad utenti con una conoscenza media di computer, questa modalità amplia le funzionalità presenti nella Modalità inesperto. È possibile risolvere problemi separatamente e scegliere quali problemi monitorare. Inoltre è possibile gestire in remoto prodotti Acronis installati su computer della propria casa.
Modalità avanzata	Adatta ad utenti esperti, questa modalità consente di configurare ogni funzionalità di Acronis Backup and Security 2010. Inoltre è possibile utilizzare tutte le attività fornite per proteggere il proprio computer e i dati.

6.3.4. Passo 4 - Configurazione Controllo Genitori

Nota

Questo passaggio appare solo se si è selezionata l'opzione **Personalizzata** nel passaggio 1.

Configurare Controllo dei Genitori

Il Controllo dei Genitori vi permette di controllare l'accesso ad Internet e ad applicazioni specifiche di ogni utente che possieda un account nel sistema.

Se volete usare il Controllo dei Genitori, seguire questi passaggi:

1. Selezionare **Abilita Controllo Genitori**.
2. Se si condivide il proprio account utente Windows con i bambini, selezionare la casella di controllo corrispondente e digitare la password nei campi corrispondenti in modo da proteggere le impostazioni di Controllo Genitori. Chiunque cerchi di modificare le impostazioni di Controllo Genitori deve innanzitutto fornire la password configurata.

Selezionare **Successivo** per continuare.

6.3.5. Passo 5 - Configurare la Rete Acronis

Nota

Questo passaggio appare solo se si è specificato che il computer è collegato ad una rete domestica al Passaggio 2.

Configurazione della Rete Domestica

Acronis Backup and Security 2010 vi permette di creare una rete virtuale con i computer della vostra famiglia e di gestire i prodotti compatibili Acronis installati nella rete.

Se vuoi che questo computer faccia parte della Rete Domestica Acronis, segui questi passi:

1. Selezionare **Abilita Rete Domestica**.

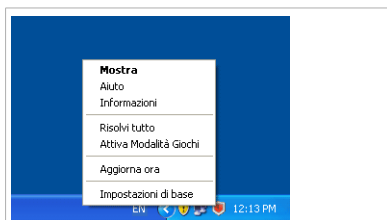
2. Inserire la stessa password di amministratore in ogni campo di modifica. La password permette ad un amministratore di gestire questo prodotto Acronis da un altro computer.

Selezionare **Termina**.

6.4. Icona barra delle applicazioni

Per gestire tutto il prodotto più velocemente, è possibile utilizzare l'icona Acronis nella barra delle applicazioni. Se si fa doppio clic su questa icona, Acronis Backup and Security 2010 si aprirà. Inoltre, facendo clic con il pulsante destro sull'icona, apparirà un menu contestuale che consentirà una rapida gestione del prodotto Acronis Backup and Security 2010.

Icona della barra delle applicazioni

- **Mostra** - apre l'interfaccia di Acronis Backup and Security 2010.
- **Aiuto** - apre il file di aiuto, che spiega nel dettaglio come configurare e usare Acronis Backup and Security 2010.
- **Informazioni** - apre una finestra nella quale è possibile visualizzare delle informazioni su Acronis Backup and Security 2010 e cercare aiuto nel caso in cui accada qualcosa di inaspettato.
- **Risolvi tutto** - aiuta a rimuovere tutte le vulnerabilità di sicurezza correnti. Se l'opzione non è disponibile, non ci sono errori da riolvere. Per ulteriori informazioni, far riferimento a *«Risolvi i Problemi»* (p. 34).
- **Modalità Gioco SI/NO** - attiva / disattiva la Modalità Gioco.
- **Aggiorna adesso** - inizia un aggiornamento immediato. Apparirà una nuova finestra, dove potrete visualizzare lo stato dell'aggiornamento.
- **Impostazioni di base** - apre una finestra dove è possibile cambiare la modalità interfaccia utente e abilitare e disabilitare il prodotto principale. Per ulteriori informazioni, far riferimento a *«Configurazione delle Impostazioni di base»* (p. 38).

L'icona Acronis nell'area di notifica fornisce informazioni relative ai problemi del computer o al funzionamento del prodotto, visualizzando un simbolo speciale come segue:

Icona rossa con un punto esclamativo: Si sono verificati dei problemi critici per la sicurezza del sistema. Tali problemi richiedono immediata attenzione e devono essere risolti il più presto possibile.
Lettera G: Il prodotto funziona inGame Mode.

Se Acronis Backup and Security 2010 non è in funzione, l'icona nell'area di notifica è disattivata. Questo si verifica normalmente quando la licenza è scaduta. Può anche verificarsi quando i servizi di Acronis Backup and Security 2010 non rispondono o quando altri errori interferiscono con il normale funzionamento di Acronis Backup and Security 2010.

6.5. Barra di Attività della Scansione

La **Barra delle attività di scansione** è una visualizzazione grafica dell'attività di scansione sul vostro sistema. Questa piccola finestra è disponibile per default solo nella Modalità Avanzata.

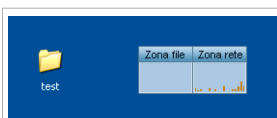
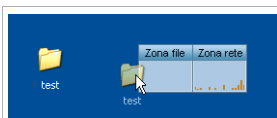
Le barre grigie (**Zona File**) indicano il numero di file esaminati al secondo, in una scala da 0 a 50. Le barre arancioni visualizzate nella **Zona Rete** mostrano il numero di Kbyte al secondo trasferiti (inviati e ricevuti da Internet), in una scala da 0 a 100.

Barra di Attività della Scansione

Nota

La Barra attività di Scansione vi avviserà con una croce rossa sopra l'area corrispondente quando la protezione in tempo reale o il Firewall sono disattivati (**Zona File** o **Zona Rete**).

6.5.1. Scansiona File e Cartelle

Puoi usare la barra di scansione per scansionare velocemente files e cartelle (trascinandoli sopra alla barra) Selezionare il file o la cartella che si desidera esaminare e trascinarla sulla **Barra delle Attività di Scansione**, come nella figura seguente.

Trascinare il file

Abbandonare il file

Appare la procedura guidata Antivirus Scan che illustra il processo di scansione. Per ulteriori informazioni sulla procedura guidata, far riferimento a *«Procedura guidata scansione antivirus»* (p. 46).

Opzioni di scansione. Le opzioni di scansione sono preconfigurate per i migliori risultati di scansione. Se vengono individuati fili infetti, Acronis Backup and Security 2010 cercherà di disinfettarli (rimuovere il codice malware). Se la disinfettazione non riesce, la procedura guidata Antivirus Scan consentirà di specificare altre azioni da intraprendere sui file infetti. Le opzioni di scansione sono standard e non è possibile modificarle.

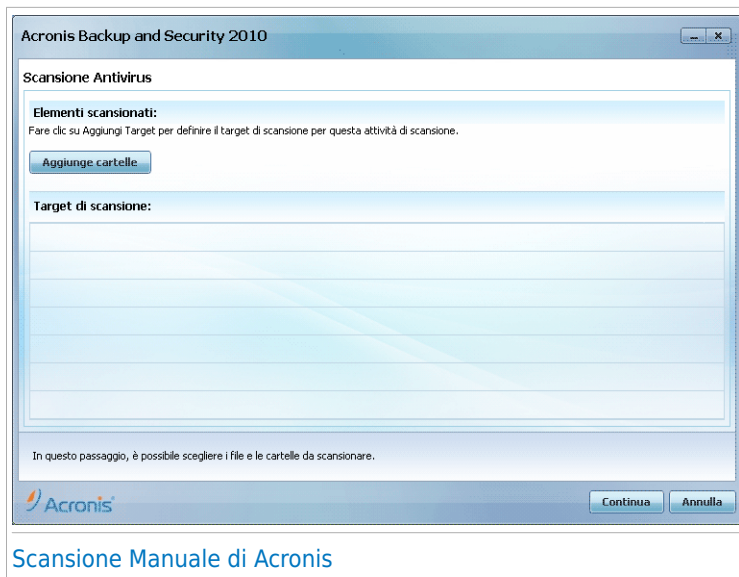
6.5.2. Disabilita/ripristina la barra di attività scansione

Quando non si vuole più vedere la visualizzazione grafica, si deve semplicemente premere sulla stessa con il pulsante destro e selezionare **Nascondi**. Per ripristinare la barra delle attività di scansione, seguire questi passi:

1. Apri Acronis Backup and Security 2010.
2. Fare clic sul pulsante **Impostazioni** in alto a destra.
3. Nella categoria Impostazioni generali, selezionare la casella di controllo corrispondente a **Barra Attività di Scansione**.
4. Fare clic su **OK** per salvare e applicare i cambiamenti.

6.6. Scansione Manuale di Acronis

La scansione Manuale Acronis consente di scansionare cartelle o partizioni di disco rigido specifiche senza dover creare una attività di scansione. Questa funzionalità è stata progettata per essere utilizzata quando Windows è in Modalità provvisoria. Se il sistema è infettato con un virus resistente, si può provare a rimuovere il virus avviando Windows nella Modalità provvisoria e eseguendo la scansione di ogni partizione di disco rigido usando Acronis Manual Scan.

Per accedere alla Scansione Manuale Acronis utilizzare il menu Avvio di Windows, seguendo il percorso **Avvio** → **Programmi** → **Acronis** → **Acronis Backup and Security 2010** → **Scansione Manuale Acronis** Apparirà la finestra seguente:

Scansione Manuale di Acronis

Fare clic su **Aggiungi Cartella**, selezionare la posizione per cui si desidera eseguire la scansione e fare clic su **OK**. Se si desidera eseguire la scansione di cartelle multiple, ripetere questa azione per ciascuna posizione aggiuntiva.

I percorsi alle posizioni selezionate appariranno nella colonna **Target di Scansione**. Se si cambia idea circa la locazione, sarà sufficiente fare clic sul pulsante **Rimuovere** vicino. Fare clic sul pulsante **Rimuovi Tutti i Percorsi** per rimuovere tutte le posizioni aggiunte all'elenco.

Quando si ha concluso la selezione delle posizioni, fare clic su **Continua**. Appare la procedura guidata Antivirus Scan che illustra il processo di scansione. Per ulteriori informazioni sulla procedura guidata, far riferimento a *«Procedura guidata scansione antivirus»* (p. 46).

Opzioni di scansione. Le opzioni di scansione sono preconfigurate per i migliori risultati di scansione. Se vengono individuati fili infetti, Acronis Backup and Security 2010 cercherà di disinfettarli (rimuovere il codice malware). Se la disinfettazione non riesce, la procedura guidata Antivirus Scan consentirà di specificare altre azioni da intraprendere sui file infetti. Le opzioni di scansione sono standard e non è possibile modificarle.

Cos'è la Modalità provvisoria?

La modalità provvisoria è un modo speciale di avviare Windows, usato principalmente per risolvere problemi che influenzano il normale funzionamento di Windows. Tali problemi vanno da driver in conflitto a virus che impediscono a Windows di avviarsi

normalmente. Nella Modalità provvisoria, Windows carica solo una parte minima di componenti del sistema operativo e dei driver fondamentali. Solo alcune applicazioni funzionano nella Modalità provvisoria. Ecco perché la maggior parte del virus sono inattivi quando si utilizza Windows nella Modalità provvisoria e perché possono essere facilmente rimossi.
Per avviare Windows nella Modalità provvisoria, riavviare il computer e premere il tasto F8 fino a quando appare il Menu opzioni avanzate di Windows. È possibile scegliere tra varie opzioni di Windows nella Modalità provvisoria. Si può selezionare **Modalità provvisoria con Networking** per abilitare l'accesso a Internet.

Nota

Per ulteriori informazioni sulla Modalità provvisoria, fare clic su Guida e Supporto tecnico di Windows (nel menu Start, fare clic su **Guida e Supporto tecnico**). È inoltre possibile trovare informazioni utili cercando su Internet.

6.7. Modalità giochi e Modalità portatile

Alcune attività del computer, ad esempio giochi o presentazioni, richiedo una maggiore risposta e performance, dal sistema e nessuna interruzione. Quando il laptop funziona a batterie, si consiglia che operazioni superflue, che consumano energia aggiuntiva, siano rimandate fino a quando il laptop è connesso all'alimentazione C/A.

Per adattarsi a queste situazioni particolari, Acronis Backup and Security 2010 include due modalità operative speciali:

- Modalità giochi
- Modalità portatile

6.7.1. Modalità giochi

La Modalità Gioco modifica temporaneamente le impostazioni di protezione in modo di minimizzare l'impatto sulle prestazioni del sistema. Mentre siete in Modalità Gioco, verranno applicate le seguenti impostazioni:

- Minimizzare il consumo di memoria e di tempo del processore.
- Posporre scansioni ed aggiornamenti automatici.
- Eliminare tutti gli allarmi ed i pop-up.
- Eseguire la scansione solo dei file più importanti.

Mentre siete in Modalità Gioco, potete vedere la lettera G sull'icona Acronis .

Uso della Modalità Gioco.

Di default, Acronis Backup and Security 2010 entra automaticamente in Modalità Gioco quando iniziate un gioco incluso nella lista dei giochi conosciuti o quando

un'applicazione passa a schermo pieno. Acronis Backup and Security 2010 tornerà automaticamente alla modalità normale quando si chiude il gioco o quando l'applicazione rilevata esce dallo schermo intero.

Se si vuole attivare manualmente la Modalità giochi, utilizzare uno dei metodi seguenti:

- fare clic con il pulsante destro sull’icona di Acronis nella barra di sistema e selezionare **Attivare Modalità giochi**.
- Premere `Ctrl+Shift+Alt+G` (la hotkey di default).

Importante

Non dimenticare di disattivare la Modalità Gioco quando avete finito. Per farlo, utilizzare gli stessi metodi usati per attivarla.

Modifica Hotkey della Modalità Gioco.

Per modificare la hotkey, seguire questi passaggi:

1. Aprire Acronis Backup and Security 2010 e passare l'interfaccia utente in Modalità Avanzata.
2. Fare clic su **Modalità giochi / portatile** nel menu a sinistra.
3. Fare clic sulla scheda **Modalità giochi**.
4. Fare clic sul pulsante **Impostazioni Avanzate**.
5. Sotto l'opzione **Usare HotKey**, impostare la hotkey desiderata:
   - Scegliere i tasti di modifica che si vogliono usare selezionando uno dei seguenti: tasto Control (`Ctrl`), tasto Maiuscola (`Shift`) o tasto Alternare (`Alt`).
   - Nel campo editabile, inserire la lettera corrispondente al tasto regolare che si vuole usare.

   Ad esempio, se volete usare la hotkey `Ctrl+Alt+D`, dovete solo controllare i tasti `Ctrl` e `Alt` ed inserire la `D`.

   Nota

   Togliere lo spunto da **Usare HotKey** disabiliterà la hotkey.
6. Selezionare **Applica** per salvare le modifiche.

6.7.2. Modalità Portatile

La Modalità Portatile è stata specialmente disegnata per chi usa i laptop/notebook. Il suo proposito è minimizzare l'impatto di Acronis Backup and Security 2010 sul consumo di energia mentre questi apparecchi funzionino con la batteria. Nella Modalità portatile, le attività di scansione programmate non vengono eseguite,

poiché richiedono più risorse di sistema e, implicitamente, un consumo di energia superiore.

Acronis Backup and Security 2010 rileva quando il vostro portatile sta funzionando con la batteria ed automaticamente va in Modalità Portatile. Nello stesso modo, Acronis Backup and Security 2010 uscirà automaticamente dalla Modalità Portatile quando rileverà che il portatile non sta più lavorando con la batteria.

Per abilitare la Modalità portatile di Acronis Backup and Security 2010, segua i seguenti passi:

1. Apri Acronis Backup and Security 2010.
2. Fare clic sul pulsante **Impostazioni** in alto a destra.
3. Nella categoria Impostazioni generali, selezionare la casella di controllo corrispondente a **Individuazione Modalità portatile**.
4. Fare clic su **OK** per salvare e applicare i cambiamenti.

6.8. Rilevamento dispositivo automatico

Acronis Backup and Security 2010 rileva automaticamente quando si collega un dispositivo rimovibile al computer e chiede di eseguirne la scansione prima che si acceda ai suoi file. Questa operazione è consigliata per impedire che virus e altri malware infettino il computer.

I dispositivi rilevati rientrano in una di queste categorie:

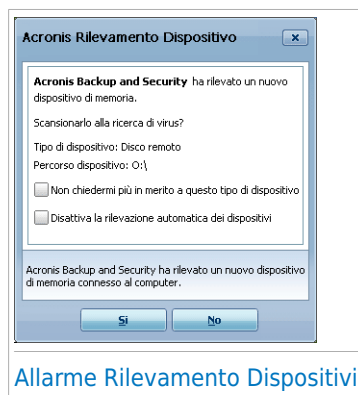
- CD/DVD
- Dispositivi di archiviazione USB, ad esempio chiavette e dischi rigidi esterni
- unità di rete (remote) mappate

Quando un tale dispositivo viene rilevato, viene visualizzata una finestra di avviso.

Per scansionare il dispositivo di archiviazione, è sufficiente fare clic su **Sì**. Appare la procedura guidata Antivirus Scan che illustra il processo di scansione. Per ulteriori informazioni sulla procedura guidata, far riferimento a *«Procedura guidata scansione antivirus»* (p. 46).

Allarme Rilevamento Dispositivi

Se non si desidera scansionare il dispositivo, si deve fare clic su **No**. In questo caso, si possono ritenere utili una di queste opzioni:

- **Non farmi più domande su questo tipo di dispositivo** - Acronis Backup and Security 2010 non chiederà più di eseguire la scansione di dispositivi di questo tipo quando sono collegati al tuo computer.

- **Disabilita rilevamento automatico dispositivi** - Non verrà più chiesto di eseguire la scansione di nuovi dispositivi di archiviazione quando sono collegati al computer.

Se per sbaglio si disabilita il rilevamento automatico dei dispositivi di archiviazione e si desidera abilitarlo, o se si desidera configurarne le impostazioni, eseguire questi passi:

1. Aprire Acronis Backup and Security 2010 e passare l'interfaccia utente in Modalità Avanzata.
2. Fare clic su **Antivirus>Virus Scan**.
3. Nell'elenco delle attività di scansione, individuare l'attività **Scansione rilevamento dispositivi**.
4. Fare clic sull'attività e selezionare **Apri**. Apparirà una nuova finestra.
5. Sulla scheda **Panoramica**, configurare le opzioni di scansione come necessarie. Per ulteriori informazioni, vi preghiamo di riferirvi a *«Configurazione delle Impostazioni di Scansione»* (p. 131).
6. Sulla scheda **Rilevamento**, scegliere i tipi di dispositivi di archiviazione da rilevare.
7. Fare clic su **OK** per salvare e applicare i cambiamenti.

7. Risolvi i Problemi

Acronis Backup and Security 2010 utilizza un sistema di identificazione dei problemi per rilevare e fornire informazioni relative ai problemi che potrebbero avere effetto sulla sicurezza del computer e dei dati. Per default il sistema controlla solo una serie di problemi considerati molto importanti. Tuttavia è possibile configurare il sistema come si desidera, scegliendo di quali problemi specifici si desidera ricevere una notifica.

I problemi in sospeso vengono notificati nel modo seguente:

- Viene visualizzato un simbolo speciale sull'icona Acronis nell'area di notifica ad indicare la presenza di problemi in sospeso.

  Icona rossa con un punto esclamativo: Si sono verificati dei problemi critici per la sicurezza del sistema. Tali problemi richiedono immediata attenzione e devono essere risolti il più presto possibile.

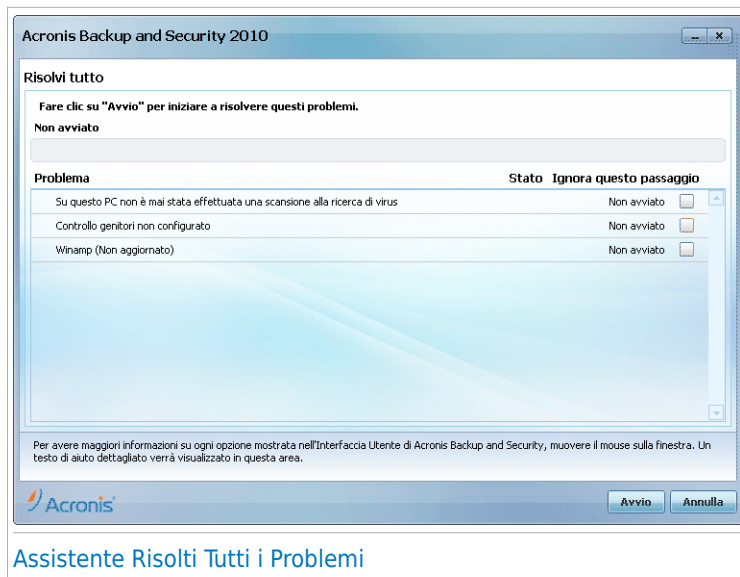
  Inoltre muovendo il cursore sull'icona un pop-up confermerà l'esistenza di problemi in sospeso.

- Quando viene aperto Acronis Backup and Security 2010, l'area Stato della Sicurezza indicherà il numero di problemi del sistema.
  - In Modalità Intermedia, lo stato della sicurezza viene visualizzato nella scheda **Dashboard**.
  - In Modalità Avanzata, andare su **Generale>Dashboard** per controllare lo stato della sicurezza.

7.1. Assistente Risolti Tutti i Problemi

Il modo più semplice di risolvere i problemi esistenti è di seguire le istruzioni passo-passo dell'assistente **Risolvi tutto**. L'assistente aiuta a rimuovere con facilità qualsiasi minaccia per la sicurezza del computer e dei dati. Per aprire l'assistente, compiere una delle seguenti operazioni:

- Fare clic con il pulsante di destra sull'icona Acronis nell'area di notifica e selezionare **Risolvi tutto**.
- Apri Acronis Backup and Security 2010. A seconda della modalità dell'interfaccia utente, procedere come segue:
  - In Modalità Inesperto, fare clic su **Risolvi tutto**.
  - In Modalità Intermedia, andare alla scheda **Dashboard** e fare clic su **Risolvi tutto**.
  - In Modalità Avanzata, andare su **Generale>Dashboard** e fare clic su **Risolvi tutto**.

Assistente Risolti Tutti i Problemi

L'assistente visualizza l'elenco delle vulnerabilità di sicurezza esistenti sul computer.

Tutti i problemi attuali sono stati selezionati per essere risolti. Se vi è un problema che non si desidera risolvere, selezionare la casella di controllo corrispondente. In questo modo lo stato cambierà su **Ignora**.

Nota

Se non si desidera ricevere notifiche relative a particolari problemi è necessario configurare di conseguenza il sistema di controllo, come descritto alla sezione successiva.

Per risolvere i problemi selezionati, fare clic su **Avvia**. Alcuni problemi vengono risolti immediatamente. Per altri problemi verrà eseguito un assistente per poterli risolvere.

I problemi che l'assistente permette di risolvere possono essere raggruppati nelle seguenti categorie principali:

- **Impostazioni di sicurezza disabilitate.** Tali problemi vengono risolti immediatamente abilitando le rispettive impostazioni di sicurezza.
- **Attività di sicurezza preventiva che è necessario eseguire.** Un esempio di tali attività è la scansione del computer. Si consiglia di eseguire la scansione del compuer almeno una volta alla settimana. Acronis Backup and Security 2010 compirà questa attività automaticamente nella maggior parte dei casi. Tuttavia

se il programma di scansione è stato modificato o non è stato completato, si riceverà un avviso relativo a questo problema.

Nel risolvere tali problemi, un assistente permette di completare con successo l'attività.

- **Vulnerabilità del sistema.** Acronis Backup and Security 2010 controlla automaticamente il sistema alla ricerca di vulnerabilità e fornisce avvisi al riguardo. Le vulnerabilità di sistema includono quanto segue:
  - password deboli per gli account utente di Windows.
  - software obsoleto sul computer.
  - aggiornamenti di Windows mancanti.
  - Gli Aggiornamenti Automatici di Windows sono disabilitati.

  Quando è necessario risolvere tali problemi, viene avviato l'assistente scansione vulnerabilità. Questo assistente permette di risolvere le vulnerabilità di sistema rilevate. Per ulteriori informazioni fare riferimento alla sezione *«Procedura guidata di Controllo delle vulnerabilità»* (p. 58).

7.2. Configurazione del monitoraggio problemi

Il sistema di controllo dei problemi è preconfigurato per il monitoraggio e l'avviso relativo ai più importanti problemi che possono influenzare la sicurezza del computer e dei dati. Ulteriori problemi possono essere monitorati in base alle scelte compiute nell'assistente di configurazione (quando viene configurato il profilo di utilizzo). Oltre ai problemi monitorati per default, vi sono molti altri problemi su cui si può essere informati.

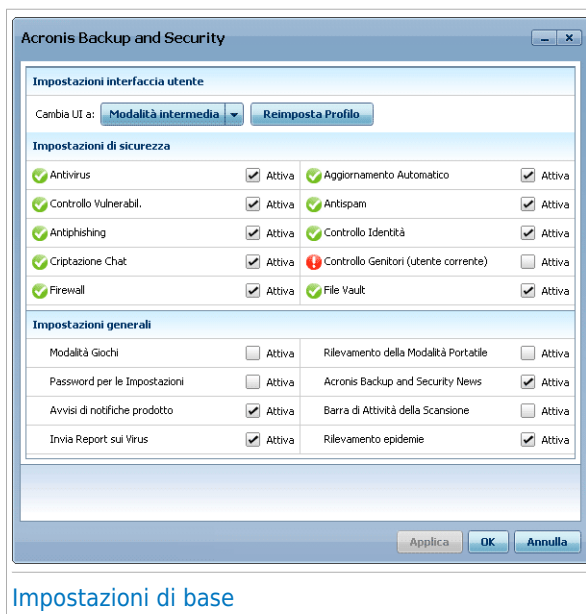
E' possibile configurare il sistema di controllo per rispondere al meglio alle proprie esigenze di sicurezza, selezionando di quali problemi specifici si desidera essere informati. Questa operazione è possibile in Modalità Intermedia o Avanzata.

- In Modalità Intermedia, il sistema di monitoraggio può essere configurato da posizioni separate. Attenersi alla seguente procedura:
  1. Andare alle schede **Sicurezza**, **Controllo Genitori** oppure **File Vault**.
  2. Fare clic su **Configura Status Alerts**.
  3. Selezionare le caselle di controllo corrispondenti agli elementi che si desidera monitorare.

  Per ulteriori informazioni, far riferimento alla parte «Modalità intermedia» (p. 84) di questo manuale.
- In Modalità Avanzata, il sistema di monitoraggio può essere configurato da una posizione centrale. Attenersi alla seguente procedura:
  1. Fare clic su **Dashboard>Generale**.
  2. Fare clic su **Configura Status Alerts**.

3. Selezionare le caselle di controllo corrispondenti agli elementi che si desidera monitorare.

Per ulteriori informazioni fare riferimento al capitolo «*Dashboard*» (p. 107).

8. Configurazione delle Impostazioni di base

È possibile configurare le impostazioni principali del prodotto (inclusa la modifica la modalità di visualizzazione dell'interfaccia utente) dalla finestra delle impostazioni fondamentali. Per aprirla, seguire una delle seguenti procedure:

- Aprire Acronis Backup and Security 2010 e fare clic sul pulsante **Impostazioni** in alto a destra.
- Fare clic con i pulsante di destra sull'icona Acronis nella barra delle applicazioni e selezionare **Impostazioni di base**.

Nota

Per configurare in dettaglio le impostazioni del prodotto, utilizzare l'interfaccia nella Modalità Avanzata. Per ulteriori informazioni, far riferimento alla parte «Modalità avanzata» (p. 106) di questo manuale.

Impostazioni di base

Le impostazioni sono suddivise in tre categorie:

- Impostazioni interfaccia utente
- Impostazioni sulla sicurezza
- Impostazioni generali

Per applicare e salvare le modifiche apportate alla configurazione, fare clic su **OK**. Per chiudere la finestra senza salvare i cambiamenti, fare clic su **Elimina**.

8.1. Impostazioni interfaccia utente

In quest'area è possibile commutare la modalità di visualizzazione dell'interfaccia utente e ripristinare il profilo di utilizzo.

Commutazione della modalità di visualizzazione dell'interfaccia utente. Come descritto nella sezione *«Modalità di visualizzazione dell'interfaccia dell'utente.»* (p. 12), ci sono tre modalità di visualizzazione dell'interfaccia utente. Ogni modalità di visualizzazione dell'interfaccia utente è progettata per una categoria specifica di utenti, in base alla loro conoscenza dei computer. In questo modo, l'interfaccia utente può soddisfare i requisiti di tutti i tipi di utenti, dai principianti agli esperti.

Il primo pulsante mostra la modalità di visualizzazione dell'interfaccia utente attuale. Per cambiare la modalità interfaccia utente, fare clic sulla freccia sul pulsante e selezionare la modalità desiderata dal menu.

Modalità	Descrizione
Modalità inesperto	Adatta per principianti e per persone che desiderano che Acronis Backup and Security 2010 protegga il proprio computer e i dati senza essere tanti problemi. Questa modalità è di facile utilizzo e richiede un intervento minimo da parte dell'utente. La sola cosa da fare è risolvere i problemi indicati da Acronis Backup and Security 2010. Una facile procedura guidata aiuterà a risolvere i problemi. Inoltre è possibile compiere attività comuni quale l'aggiornamento delle firme dei virus di Acronis Backup and Security 2010 e dei file del prodotto, oppure la scansione del computer.
Modalità intermedia	Rivolta ad utenti con una conoscenza media di computer, questa modalità amplia le funzionalità presenti nella Modalità inesperto. È possibile risolvere problemi separatamente e scegliere quali problemi monitorare. Inoltre è possibile gestire in remoto prodotti Acronis installati su computer della propria casa.
Modalità Avanzata	Adatta ad utenti esperti, questa modalità consente di configurare ogni funzionalità di Acronis Backup and Security 2010. Inoltre è possibile utilizzare tutte le

Modalità	Descrizione
	attività fornite per proteggere il proprio computer e i dati.

Riconfigurazione del profilo di utilizzo. Il profilo di utilizzo rispecchia le attività principali eseguite sul computer. A seconda del profilo di utilizzo, l'interfaccia del prodotto è organizzata in modo da permettere facile accesso alle attività preferite.

Per riconfigurare il profilo di utilizzo, fare clic su **Reimposta Profilo** e seguire l'assistente di configurazione.

8.2. Impostazioni di sicurezza

In questa area, è possibile abilitare o disabilitare le impostazioni del prodotto che riguardano vari aspetti della sicurezza del computer e dei dati. Lo stato attuale delle impostazioni è indicato usando una di queste icone:

Cerchio verde con un segno di spunta: L'impostazione è abilitata.

Cerchio rosso con un punto esclamativo: L'impostazione è disabilitata.

Per abilitare / disabilitare una impostazione, selezionare / deselezionare la casella di controllo **Abilita** corrispondente.

Avvertimento

Prestare molta attenzione prima di disabilitare la protezione antivirus in tempo reale, il firewall o aggiornamenti automatici. Disabilitare queste funzionalità potrebbe compromettere la sicurezza del proprio computer. Se è davvero necessario disabilitarle, ricordarsi di riabilitarle appena possibile.

È possibile trovare tutto l'elenco delle impostazioni e la relativa descrizione nella seguente tabella:

Impostazione	Descrizione
Antivirus	La protezione in tempo reale assicura che tutti i file vengano scansionati quando l'utente o un'applicazione eseguita nel sistema vi accede.
Aggiornamento automatico	L'aggiornamento automatico assicura che la versione più recente del prodotto Acronis Backup and Security 2010 e i file di firma vengano scaricati ed installati automaticamente e regolarmente.
Controllo Vulnerabilità	Il controllo automatico delle Vulnerabilità assicura che il software cruciale del computer sia aggiornato.

Impostazione	Descrizione
Antispam	Antispam filtra messaggi e-mail che si ricevono, segnando posta non sollecitata e indesiderata come SPAM.
Antiphishing	L'Antiphishing rileva se una pagina web è impostata per rubare informazioni personali e avverte in tempo reale.
Controllo Identità	Il Controllo identità consente di impedire la diffusione dei propri dati personali su Internet senza il proprio consenso. Impedisce che messaggi immediati, e-mail o moduli web trasmettano dati definiti come privati a destinatari (indirizzi) non autorizzati.
Criptazione dell'IM	La Criptazione IM (Instant Messaging) rende sicure le conversazioni via Yahoo! Messenger e Windows Live Messenger a patto che i contatti IM usino un prodotto compatibile con Acronis e software IM.
Controllo dei Genitori	Il Controllo genitori restringe le attività del computer e on-line dei vostri bambini in base alle regole definite. Le restrizioni possono includere bloccare siti web inappropriati, oltre a limitare giochi e accesso a Internet in base all'orario specificato.
Firewall	Il Firewall protegge il vostro computer dagli hacker e dagli attacchi esterni.
Criptazione File	La Criptazione File mantiene al sicuro i documenti mediante la criptazione in speciali unità protette. Se disabilitate la Criptazione File, tutti i file vault verranno bloccati e non potrete più accedere ai file che li contengono.

Lo stato di alcune di queste impostazioni può essere monitorato dal sistema dicontrollo dei problemi di Acronis Backup and Security 2010. Se viene disabilitata una impostazione controllata, Acronis Backup and Security 2010 segnalerà un problema che deve essere risolto.

Se non si desidera che le impostazioni di monitoraggio disabilitate vengano indicate come problemi, è necessario configurare di conseguenza il sistema di monitoraggio. È possibile far ciò nella Modalità Intermedia o Avanzata.

- In Modalità Intermedia, il sistema di monitoraggio è configurato da posizioni separate, a seconda delle categorie di impostazioni. Per ulteriori informazioni, far riferimento alla parte «Modalità intermedia» (p. 84) di questo manuale.

- In Modalità Avanzata, il sistema di monitoraggio può essere configurato da una posizione centrale. Attenersi alla seguente procedura:
  1. Fare clic su **Dashboard>Generale**.
  2. Fare clic su **Configura Status Alerts**.
  3. Deselezionare la casella di spunta corrispondente alle voci che non si desidera monitorare.

  Per ulteriori informazioni fare riferimento al capitolo «*Dashboard*» (p. 107).

8.3. Impostazioni generali

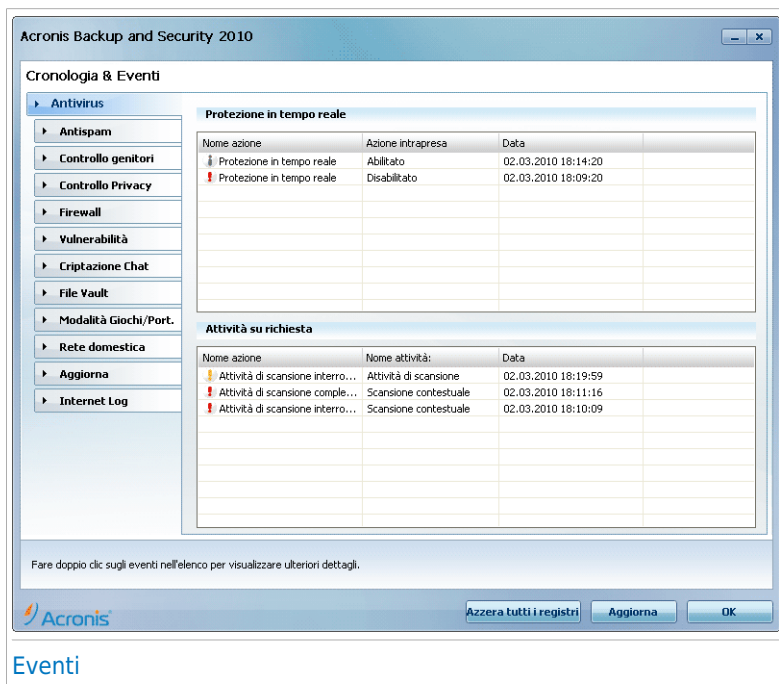
In questa area, è possibile abilitare o disabilitare impostazioni che influenzano il comportamento del prodotto e l'esperienza utente. Per abilitare / disabilitare una impostazione, selezionare / deselezionare la casella di controllo **Abilita** corrispondente.

È possibile trovare tutto l'elenco delle impostazioni e la relativa descrizione nella seguente tabella:

Impostazione	Descrizione
Modalità Gioco	La Modalità giochi modifica temporaneamente le impostazioni di protezione in modo da minimizzare il loro impatto sulle performance del sistema durante le sessioni di gioco.
Rilevamento Modalità portatile	La Modalità Portatile modifica temporaneamente le impostazioni di protezione in modo da minimizzare il loro impatto sulla durata della batteria del computer portatile.
Password delle impostazioni	Questo assicura che le impostazioni di Acronis Backup and Security 2010 possano essere modificate solo da una persona che conosca questa password. Quando viene abilitata questa opzione verrà richiesto di configurare la password impostazioni. Digitare la password desiderata in entrambi i campi e fare clic su **OK** per impostare la password.
Acronis Backup and Security News	Abilitando questa opzione, riceverete da Acronis importanti notizie sull'azienda, aggiornamenti del prodotto e notizie sulle nuove minacce per la sicurezza.
Avvisi notifiche prodotto	Abilitando questa opzione riceverete informazioni sugli allarmi.
Barra dell'Attività di scansione	La Barra dell'attività di scansione è una piccola finestra trasparente che indica l'avanzamento dell'attività

Impostazione	Descrizione
	dell'attività di scansione di Acronis Backup and Security 2010. Per ulteriori informazioni, far riferimento a *«Barra di Attività della Scansione»* (p. 27).
Inviare report sui Virus	Abilitando questa opzione i report sulle scansioni antivirus verranno inviati ai Laboratori Acronis per analisi. Questi report non contengono dati confidenziali, come il vostro nome o indirizzo IP, e non verranno usati a fini commerciali.
Rilevamento di Outbreak	Abilitando questa opzione i report riguardanti potenziali outbreak di virus verranno inviati ai Laboratori Acronis per analisi. Questi report non contengono dati confidenziali, come il vostro nome o indirizzo IP, e non verranno usati a fini commerciali.

9. Cronologia ed Eventi

Il link **Registri** nella parte inferiore della finestra principale di Acronis Backup and Security 2010 apre un'altra finestra che visualizza la cronologia e gli eventi di Acronis Backup and Security 2010. Tale finestra offre una panoramica di tutti gli eventi relativi alla sicurezza. Per esempio, potete potete controllare facilmente se l'aggiornamento è stato eseguito con successo, se è stato rilevato del malware sul vostro computer, etc.

Eventi

Per aiutarvi a filtrare la cronologia ed eventi di Acronis Backup and Security 2010, sulla sinistra sono disponibili le seguenti categorie:

- **Antivirus**
- **Antispam**
- **Controllo dei Genitori**
- **Controllo della Privacy**
- **Firewall**
- **Vulnerabilità**
- **Criptazione IM**
- **Criptazione File**

- **Modalità portatile/giochi**
- **Rete Domestica**
- **Aggiornamento**
- **Registro Internet**

Per ogni categoria c'è una lista di eventi disponibile. Ogni evento viene con la seguente informazione: una breve descrizione, l'azione intrapresa da Acronis Backup and Security 2010 quando è successo, e la data ed ora in cui è successo. Se volete trovare ulteriori informazioni su un particolare evento della lista, cliccateci due volte sopra.

Fare clic su **Cancella tutti i registri** se si desidera rimuovere tutti i vecchi registri, oppure **Aggiorna** per assicurarsi di visualizzare i registri più recenti.

10. Procedure guidate

Per facilitare l'uso di Acronis Backup and Security 2010, diverse procedure guidate aiutano a svolgere specifiche attività di sicurezza o configurare impostazioni del prodotto più complesse. Questa capitolo descrive le procedure guidate potrebbero apparire quando si risolvono problemi o svolgono attività specifiche con Acronis Backup and Security 2010. Altre procedure guidate di configurazione sono descritte separatamente nella parte «Modalità avanzata» (p. 106).

10.1. Procedura guidata scansione antivirus

Ogni volta che si inizia una scansione su richiesta (ad esempio, facendo clic con il tasto destro su una cartella e selezionando **Scansiona con Acronis Backup and Security**), apparirà l'assistente Scansione Antivirus. Seguire la procedura di tre passi per completare il processo di scansione.

Nota

Se non appare la procedura guidata di scansione, potrebbe darsi che la procedura guidata sia configurata per una esecuzione sullo sfondo. Cercare l'icona di avanzamento della scansione nella barra delle applicazioni. Clicca su questa icona per aprire un processo di scansione e visualizzarne il progresso.

10.1.1. Passo 1/3 – Scansione

Acronis Backup and Security 2010 inizierà la scansione degli oggetti selezionati.

Scansione in corso

Potete visualizzare lo stato della scansione e le statistiche (velocità di scansione, tempo trascorso, numero di oggetti esaminati / infetti / sospetti / nascosti ed altro).

Attendere che Acronis Backup and Security 2010 finisca la scansione.

Nota
La durata del processo dipende dalla complessità della scansione.

Archivi protetti da password. Se Acronis Backup and Security 2010 rileva un archivio protetto da password durante la scansione e l'azione predefinita è **Richiedi la password**, verrà chiesto di inserire la password. Gli archivi protetti da password non possono essere esaminati a meno che non forniate la password. Sono disponibili le seguenti opzioni:

- **Desidero inserire la password per questo oggetto.** Se si desidera che Acronis Backup and Security 2010 scansioni l'archivio, selezionare questa opzione e digitare la password. Se non si conosce la password, scegliere un'altra opzione.
- **Non desidero inserire la password per questo oggetto (ignora questo oggetto).** Selezionare questa opzione per non scansionare questo archivio.
- **Non desidero inserire la password per questi oggetti (ignora tutti gli oggetti protetti da password).** Selezionare questa opzione se non si vuole ricevere ulteriore domande sugli archivi protetti da password. Acronis Backup

and Security 2010 non sarà in grado di scansionarli, ma verranno annotati nel registro della scansione.

Fare clic su **OK** per continuare la scansione.

Arresto o messa in pausa della scansione. Potete fermare la scansione in qualsiasi momento, cliccando su **Fermare**. Verrete portati all'ultimo passo dell'assistente. Per interrompere temporaneamente il processo di scansione, cliccare semplicemente su **Pausa**. Per riprendere la scansione dovrete cliccare su **Continuare**.

10.1.2. Passo 2/3 – Selezionare Azioni

Una volta completato il processo di scansione, apparirà una nuova finestra, dove potrete visualizzare i risultati della scansione.

Azioni

Si potrà vedere il numero di problemi che colpiscono il vs. sistema.

Gli oggetti infetti vengono mostrati in gruppi in base al malware con il quale sono stati infettati. Cliccare sul link corrispondente alla minaccia per trovare più informazioni sugli oggetti infetti.

Potete scegliere di intraprendere un'azione globale per tutti i problemi oppure selezionare azioni separate per ogni gruppo di problemi.

Una o più delle seguenti opzioni possono apparire nel menu:

Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file rilevati. Dopo che la scansione sia stata completata, potrete aprire il log di scansione per visualizzare le informazioni su questi file.
Disinfettare	Rimuove il codice malware da file infetti.
Eliminare	Elimina i file infetti.
Sposta in quarantena	Sposta i file infetti nella quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.
Rinomina i files	Cambia il nome di file nascosti aggiungendo `.bd.ren` al loro nome. Come risultato, si potrà cercare tali file sul computer, se ve ne sono. Notare che i file nascosti non sono i file che l'utente ha nascosto in modo deliberato da Windows. Sono file nascosti da programmi speciali, noti come rootkit. I rootkit non sono file di tipo nocivo. Tuttavia sono utilizzati per rendere introvabili virus o spyware per normali programmi antivirus.

Cliccare su **Continuare** per applicare le azioni specificate.

10.1.3. Passo 3/3 – Visualizzare risultati

Quando Acronis Backup and Security 2010 completa la risoluzione dei problemi, i risultati della scansione appariranno in una nuova finestra.

Riassunto

E' possibile visualizzare il sommario dei risultati. Se si desiderano informazioni esaurienti sul processo di scansione, fare clic su **Visualizza registro** per visualizzare il registro di scansione.

Importante

Se richiesto, vi preghiamo di riavviare il sistema per completare il processo di pulizia.

Cliccare su **Chiudere** per chiudere la finestra.

Acronis Backup and Security 2010 potrebbe non risolvere alcuni problemi

Nella maggior parte dei casi Acronis Backup and Security 2010 disinfetta con successo i file infetti che rileva o isola l'infezione. Comunque, ci sono dei problemi che non possono essere risolti.

In questi casi vi consigliamo di contattare il Team di supporto di Acronis su http://www.acronis.it/support/?ow=1. Il nostro team di supporto vi aiuterà a risolvere i vostri problemi.

Acronis Backup and Security 2010 ha rilevato dei file sospetti

I file sospetti sono file rilevati dall'analisi euristica come potenzialmente infetti con malware la cui firma non è ancora stata rilasciata.

Se sono stati rilevati file sospetti durante la scansione, vi sarà richiesto di inviarli al Lab Acronis. Cliccare su **OK** per inviare questi file ai laboratori Acronis per ulteriori analisi.

10.2. Assistente Scansione Personalizzata

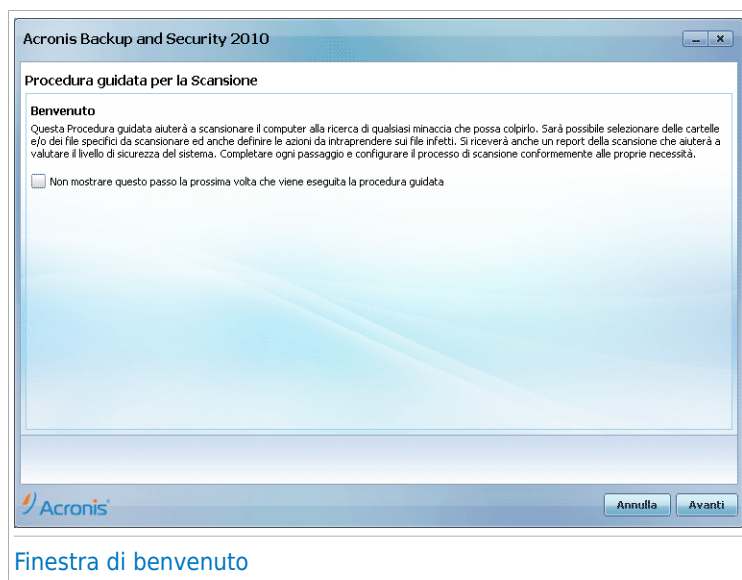
L'Assistente Scansione Personalizzata vi permette di creare ed eseguire un'attività di scansione personalizzata e di salvarla opzionamente come Attività Veloce quando si utilizza Acronis Backup and Security 2010 in Modalità Intermedia.

Per eseguire un'attività di scansione personalizzata utilizzando l'Assistente Scansione Personalizzata, è necessario seguire questi passi:

1. In Modalità Intermedia, andare alla scheda **Sicurezza**.
2. Nell'area Funzioni Rapide, clicca **Scansione Personalizzata**.
3. Seguire i sei passi della procedura guidata per completare il processo di scansione.

10.2.1. Passo 1/6 - Finestra di Benvenuto

Questa è una finestra di benvenuto.

Finestra di benvenuto

Se si desidera ignorare questa finestra quando si esegue di nuovo l'assistente in futuro, selezionare la casella di controllo **Non mostrare questo passo la prossima volta che viene eseguito l'assistente**.

Selezionare **Avanti**.

10.2.2. Passo 2/6 - Selezionare Target

Qui è possibile specificare i file o le cartelle da scansionare, nonché le opzioni di scansione.

Selezionare Target

Fare clic su **Aggiungere Target**, selezionare i file o le cartelle che si desidera scansionare e fare clic su **OK**. I percorsi alle posizioni selezionate appariranno nella colonna **Target di scansione**. Se si cambia idea circa la locazione, sarà sufficiente fare clic sul pulsante **Rimuovere** vicino. Fare clic sul pulsante **Rimuovi Tutto** per rimuovere tutte le posizioni aggiunte all'elenco.

Quando si è conclusa la selezione delle posizioni, impostare le **Opzioni di Scansione**. Sono disponibili le seguenti opzioni:

Opzione	Descrizione
Tutti i file	Selezionare questa opzione per esaminare tutti i file nelle cartelle desiderate.
Scansiona solo i file con estensioni di applicazione	Verranno esaminati solo i file di programma. Questo significa solo i file con le seguenti estensioni: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`;

Opzione	Descrizione
	.hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml e .nws.
Esamina solo le estensioni definite dall'utente	Verranno esaminati soltanto i file con le estensioni specificate dall’utente. Le varie estensioni devono essere separate da “;”.

Selezionare **Avanti**.

10.2.3. Passo 3/6 - Selezionare Azioni

Qui è possibile specificare le impostazioni dello scanner e il livello di scansione.

Selezionare Azioni

- Selezionare le azioni da intraprendere sui file infetti e sospetti rilevati. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file infetti. Questi file appariranno nel file di rapporto.

Azione	Descrizione
Disinfetta i file	Rimuovere il codice malware dai file infetti rilevati.
Cancella i file	Cancella immediatamente i file infetti, senza alcun avviso.
Muova i files in Quarantena	Sposta i file infetti nella zona di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.

- Selezionare l'azione da intraprendere sui file nascosti (rootkit). Sono disponibili le seguenti opzioni:

Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file nascosti. Questi file appariranno nel file di report.
Rinomina	Cambia il nome di file nascosti aggiungendo `.bd.ren` al loro nome. Come risultato, si potrà cercare tali file sul computer, se ve ne sono.

- Configurare l'aggessività dello scanner. Vi sono 3 livelli da cui scegliere. Trascinare il selettore lungo la scala per impostare il livello di protezione più adeguato:

Livello di scansione	Descrizione
Permissiva	Vengono esaminate solo le applicazioni e solo alla ricerca di virus. Il livello di consumo delle risorse è basso.
Default	Il livello di consumo delle risorse è moderato. Vengono analizzati tutti i file alla ricerca di virus e spyware.
Aggressiva	Vengono esaminati tutti i file (inclusi gli archivi) alla ricerca di virus e spyware. I file nascosti e i processi sono inclusi nella scansione. Il livello di consumo delle risorse è elevato.

Gli utenti più esperti possono trarre vantaggio dalle impostazioni di scansione offerte da Acronis Backup and Security 2010. Lo scanner può essere impostato per la ricerca di minacce malware specifiche. Questo può ridurre considerevolmente i tempi di scansione e migliorare i tempi di risposta del computer durante la scansione.

Trascinare il selettore per selezionare **Personalizzazione** quindi fare clic sul pulsante **Livello di Personalizzazione**. Apparirà una finestra. Specificare il tipo di malware per cui si desidera che Acronis Backup and Security 2010 compia una scansione selezionando le opzioni appropriate:

Opzione	Descrizione
Scansione Virus	Esamina per virus conosciuti. Acronis Backup and Security 2010 rileva anche virus incompleti, rimuovendo ogni possibile minaccia che possa colpire la sicurezza del vostro sistema.
Scansione adware	Esegue la scansione per minacce adware. Questi file verranno trattati come file infetti. Software che includono componenti adware potrebbero bloccarsi se questa opzione è attiva.
Scansione spyware	Esegue la scansione per minacce spyware conosciuti. Questi file verranno trattati come file infetti.
Scansiona alla ricerca di applicazioni	Cerca applicazioni legittime che possono essere usate come strumenti per spiare, per nascondere applicazioni maligne o per altri intenti maligni.
Scansione dialers	Esegue la scansione per applicazioni che utilizzano numeri di telefono a costo elevato. Questi file verranno trattati come file infetti. Software che includono componenti dialer potrebbero bloccarsi se questa opzione fosse attiva.
Scansione per i Rootkits	Esegue la scansione per oggetti nascosti (file e processi), generalmente conosciuti come rootkits.
Scansiona alla ricerca di keylogger	Scansiona applicazioni malevole che registrano i tasti premuti.

Selezionare **OK** per chiudere la finestra.

Selezionare **Avanti**.

10.2.4. Passo 4/6 - Impostazioni Aggiuntive

Prima dell'avvio della scansione sono disponibili alcune opzioni aggiuntive:

Impostazioni Aggiuntive

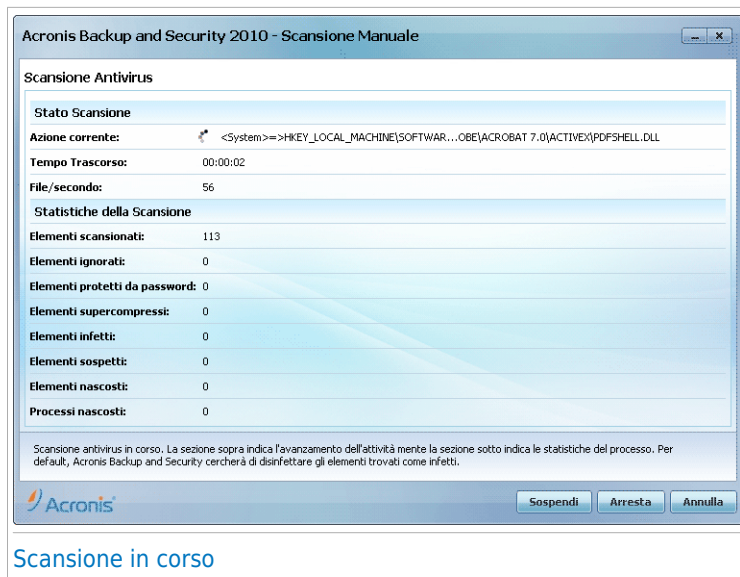
- Per salvare l'attività personalizzata che si sta creando per l'uso in futuro, selezionare la casella di controllo **Mostra questa attività nell'Interfaccia Utente Intermedia** ed inserire il nome dell'attività nel campo di immissione fornito.

  L'attività verra aggiunta all'elenco di Attività Veloci disponibile alla scheda Sicurezza e apparirà anche in **Modalità Avanzata > Antivirus > Scansione Virus**.
- Dal menù corrispondente, selezioni l'azione da intraprendere nel caso non siano state riscontrate minacce.

Fare clic su **Avvia Scansione**.

10.2.5. Passo 5/6 - Scansione

Acronis Backup and Security 2010 inizierà la scansione degli oggetti selezionati:

Scansione in corso

Nota

La durata del processo dipende dalla complessità della scansione. Facendo clic sull'icona di avanzamento della scansione nell'area di notifica si aprirà la finestra di scansione e sarà possibile osservare l'avanzamento della scansione.

10.2.6. Passo 6/6 – Visualizzare Risultati

Quando Acronis Backup and Security 2010 completa il processo di scansione, i risultati della scansione verranno visualizzati in una nuova finestra:

Riassunto

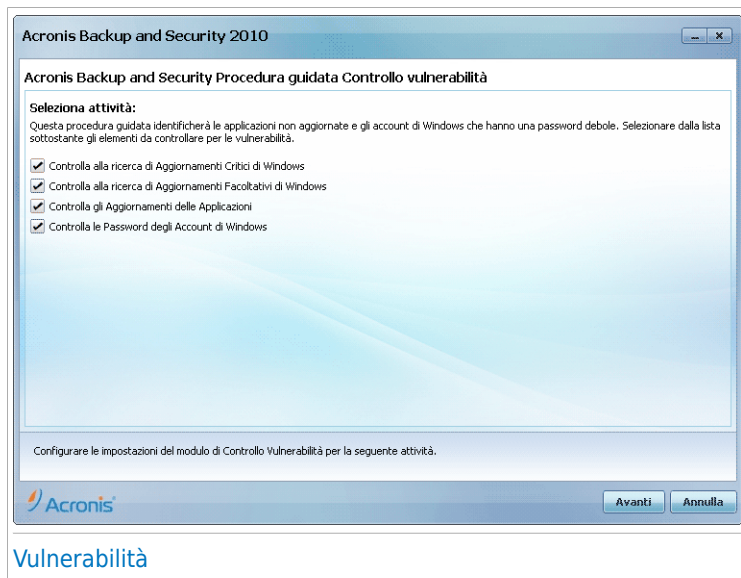
Viene visualizzato il riepilogo dei risultati. Se si desiderano informazioni esaurienti sul processo di scansione, fare clic su **Visualizza Registro** per visualizzare il registro di scansione.

Importante
Se richiesto, vi preghiamo di riavviare il sistema per completare il processo di pulizia.

Cliccare su **Chiudere** per chiudere la finestra.

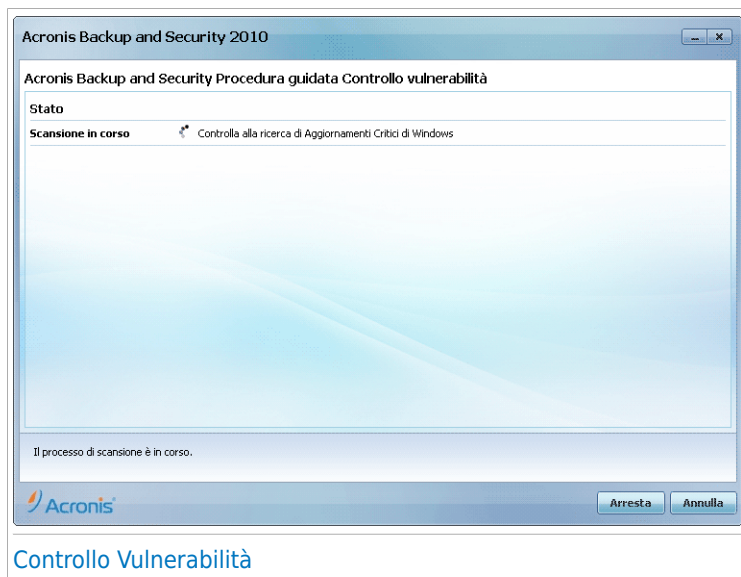
10.3. Procedura guidata di Controllo delle vulnerabilità

L'assistente controlla le vulnerabilità del sistema e permette di risolverle.

10.3.1. Passo 1/6 – Selezionare le Vulnerabilità da controllare.

Vulnerabilità

Cliccare su **Avanti** per esaminare il sistema alla ricerca delle vulnerabilità selezionate.

10.3.2. Passo 2/6 - Controllare Vulnerabilità

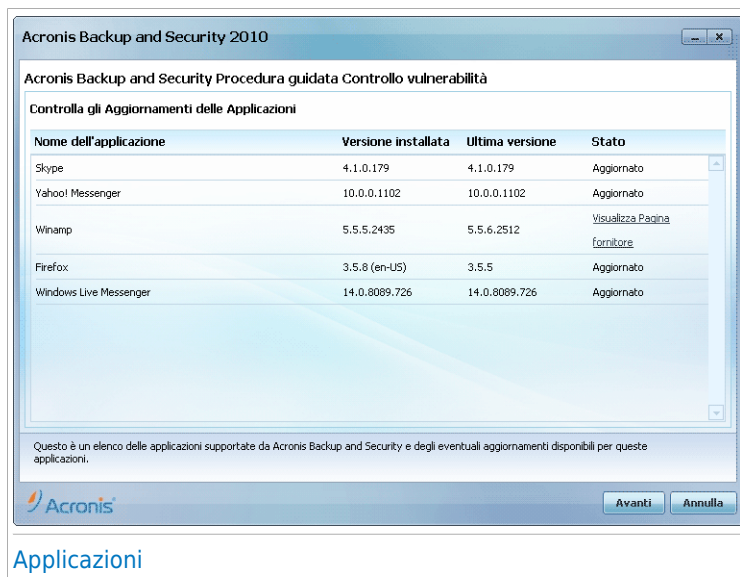
Controllo Vulnerabilità

Attendere che Acronis Backup and Security 2010 finisca il controllo alla ricerca di vulnerabilità.

10.3.3. Passo 3/6 - Aggiornare Windows

Aggiornamenti di Windows

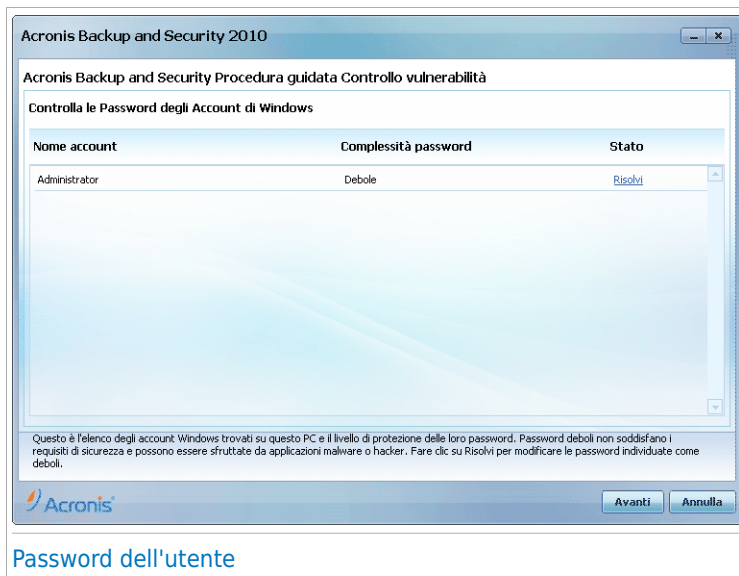
Potete vedere l'elenco degli aggiornamenti critici e non critici di Windos che non sono attualmente installati sul computer. Clicare su **Installare tutti gli aggiornamenti di sistema** per installare tutti gli aggiornamenti disponibili.

Selezionare **Avanti**.

10.3.4. Passo 4/6 - Aggiornare le Applicazioni

Applicazioni

Potete vedere l'elenco di tutte le applicazioni controllate da Acronis Backup and Security 2010 e se sono aggiornate. Se un'applicazione non è aggiornata, cliccare sul link fornito per scaricare la versione più recente.

Selezionare **Avanti**.

10.3.5. Passo 5/6 - Cambiare password deboli

Password dell'utente

Potete visualizzare l'elenco degli account di Windows configurati sul vostro computer ed il livello di protezione che le loro password forniscono. Una password può essere **forte** (difficile da indovinare) o **debole** (facile da indovinare da persone malvagie con software specializzati).

Cliccare su **Risolvere** per modificare le password deboli. Apparirà una nuova finestra.

Cambia la password

Selezionare il metodo per risolvere questo problema:

- **Forza l'utente a cambiare password al prossimo accesso.** Acronis Backup and Security 2010 chiederà l'utente di cambiare la password la prossima volta che acceda a Windows.
- **Cambia password dell'utente.** Devi inserire la nuova password nei campi corrispondenti. Assicurarsi di informare l'utente in merito al cambiamento della password.

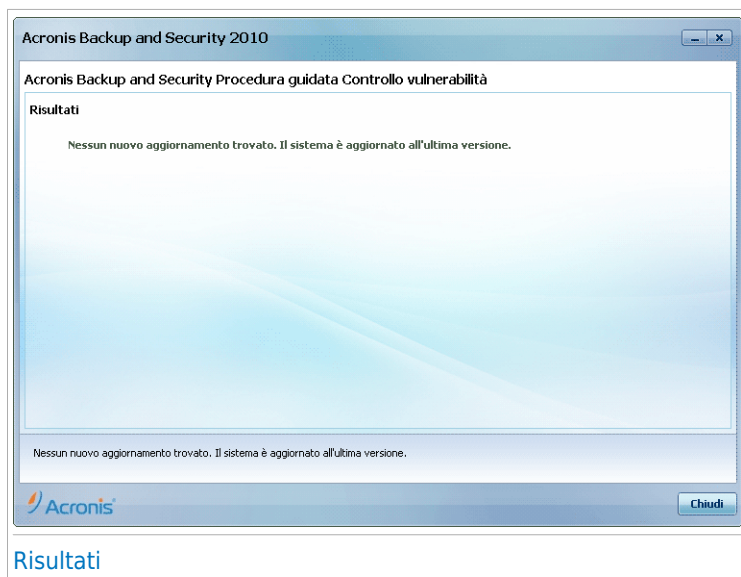
Nota

Per avere una password forte, utilizzare una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, $ o @). È possibile eseguire una ricerca su Internet per ulteriori informazioni e consigli sul creare forti password.

Cliccare su **OK** per cambiare la password.

Selezionare **Avanti**.

10.3.6. Passo 6/6 – Visualizzare Risultati

Risultati

Cliccare su **Chiudere**.

10.4. Assistente File Vault

L'assistente File Vault permette di creare e gestire i file vault di Acronis Backup and Security 2010. Un file vault è uno spazio di memorizzazione criptato sul computer, dove i file, i documenti e perfino intere cartelle possono essere conservati in sicurezza.

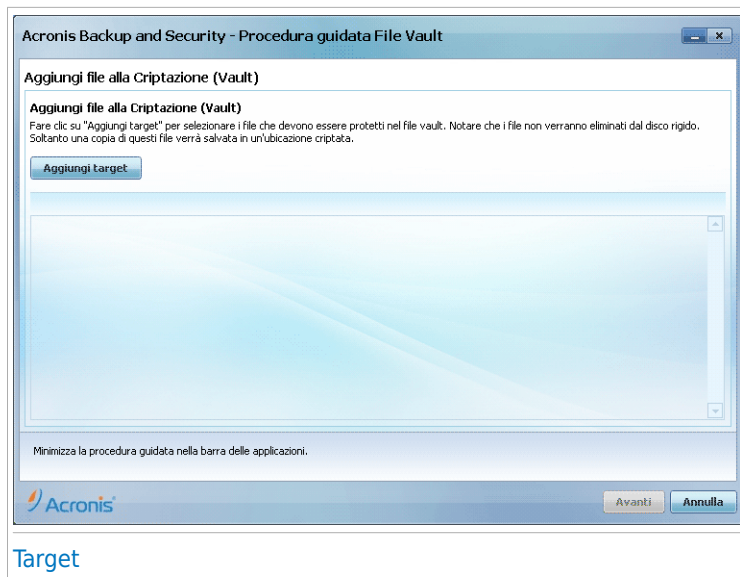
Questi assistenti non appaiono quando vengono risolti i problemi, poiché i file vault sono un metodo opzionale di protezione dei dati. Possono essere avviati solo dall'interfaccia Modalità Intermedia di Acronis Backup and Security 2010, alla scheda **Archiviazione File**, nel modo seguente:

- **Aggiungere File alla Criptazione** - inizia la procedura guidata che vi permette di immagazzinare i vostri file / documenti importanti privatamente mediante la loro criptazione in speciali drive protetti.
- **Rimuovere File dalla Criptazione** - inizia la procedura guidata che vi permette di cancellare dati dai file prottetti.
- **Visualizzare File Vault** - inizia la procedura guidata che vi permette di visualizzare il contenuto dei file vault.
- **Bloccare File Vault** - inizia la procedura guidata che permette di bloccare un file vault aperto per proteggere il suo contenuto.

10.4.1. Aggiungi file alla Criptazione (Vault)

Questo assistente permette di creare un file vault e aggiungere file ad esso per memorizzarli in sicurezza sul computer.

Passo 1/6 - Selezionare Target

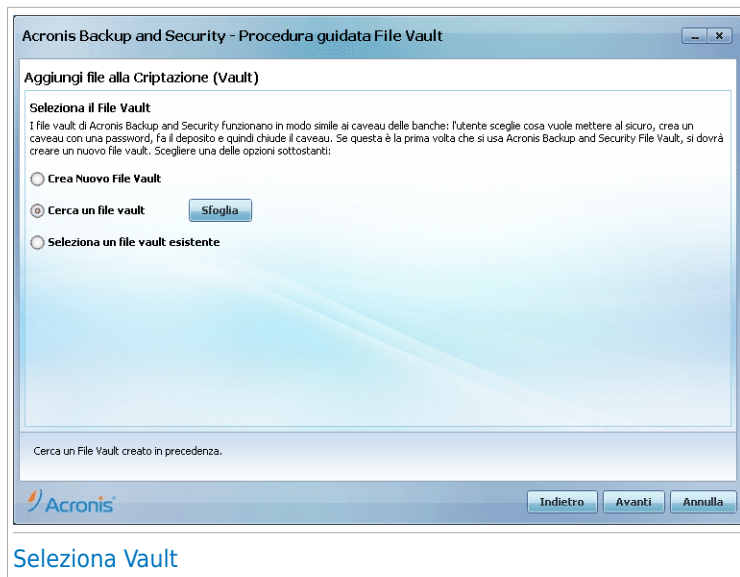
Qua potete specificare i file o cartelle da aggiungere al vault.

Target

Cliccare su **Aggiungere Target**, selezionare il file o la cartella che si vuole aggiungere e cliccare **OK**. Il percorso all'ubicazione selezionata apparirà nella colonna **Percorso**. Se si cambia idea circa la locazione, sarà sufficiente fare clic sul pulsante **Rimuovere** vicino.

Nota
E' possibile selezionare una o più ubicazioni.

Selezionare **Avanti**.

Passo 2/6 - Selezionare Vault

Qui potete creare un nuovo vault o scegliere uno esistente.

Seleziona Vault

Se selezionate **Trovare un Vault File**, dovete cliccare su **Sfoglia** e selezionare il vault. Dovrete andare al passo 5 se il vault selezionato è aperto (montato) o al passo 4 se è bloccato (smontato).

Se cliccate su **Selezionare un Vault esistente**, dovrete poi cliccare sul nome del vault desiderato. Dovrete andare al passo 5 se il vault selezionato è aperto (montato) o al passo 4 se è bloccato (smontato).

Selezionare **Creare Nuovo Vault File** se nessuno di quelli esistenti si adatta alle vostre necessità. Andrete quindi al passo 3.

Selezionare **Avanti**.

Passo 3/6 - Creare Vault

Qui è dove potrete specificare le linformazioni per il nuovo Vault.

Crea Vault

Per completare l'informazione relativa al vault, seguire questi passaggi:

1. Cliccare su **Sfoglia** e scegliere una destinazione per il file bvd.

Nota

Ricordare che il vault file è un file criptato sul vostro computer con estensione bvd.

2. Selezionare la lettera del drive per il nuovo file criptato dal corrispondente menu a tendina.

Nota

Ricordare che quando montate il file bvd, apparirà una nuova partizione logica (un nuovo drive).

3. Digitare una password per la criptazione del file nel campo corrispondente.

Nota

La password deve essere composta da almeno 8 caratteri.

4. Re-inserire la password.
5. Impostare la dimensione del vault (in MB) digitando un numero nel campo corrispondente.

Selezionare **Avanti**.

Andrete al passo 5.

Passo 4/6 – Password

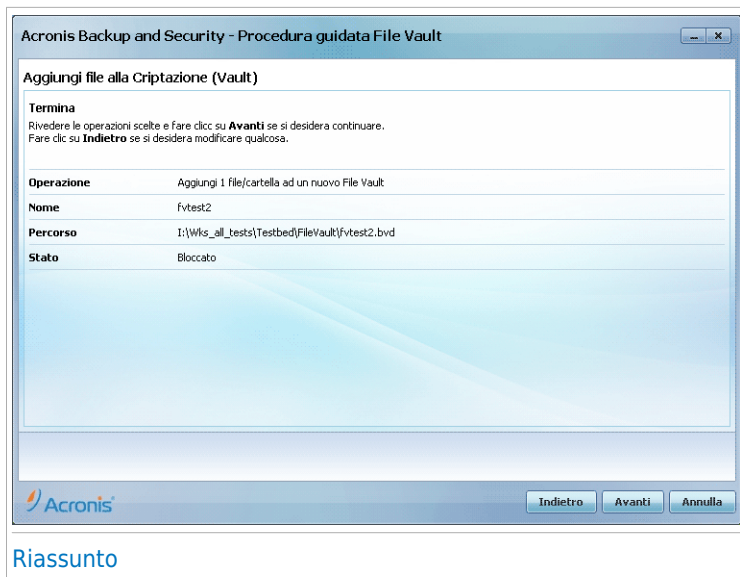
Qui è dove vi verrà chiesto di inserire la password per il vault selezionato.

Conferma password

Digitare la password nel campo corrispondente e cliccare su **Avanti**.

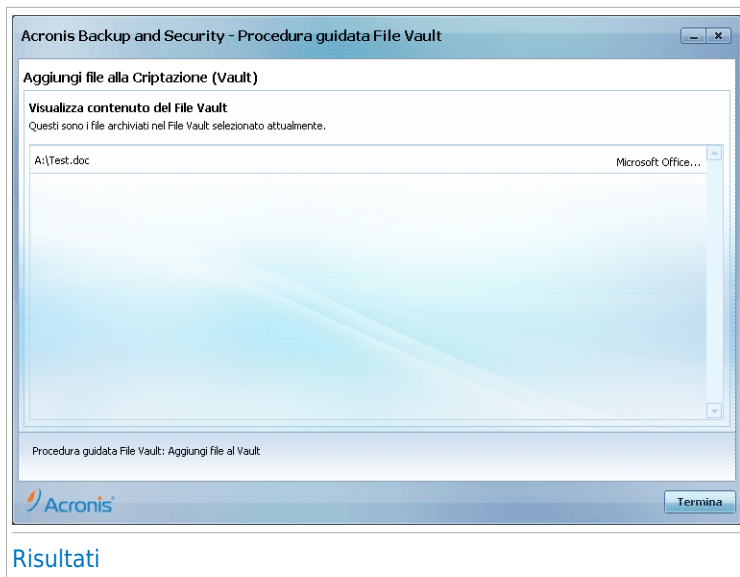
Passo 5/6 – Sommario

Qui è dove potrete rivedere le operazioni selezionate.

Riassunto

Selezionare **Avanti**.

Passo 6/6 – Risultati

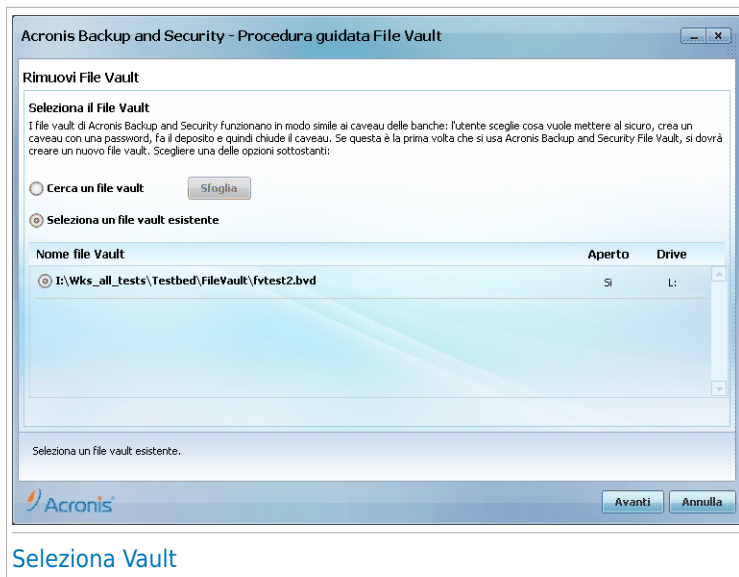
Qui è dove potete vedere il contenuto del vault.

Risultati

Selezionare **Termina**.

10.4.2. Rimuovi Vault File

Questo assistente permette di rimuovere file da uno specifico file vault.

Passo 1/5 - Selezionare Vault

Qui potete specificare il vault dal quale rimuovere i file.

Seleziona Vault

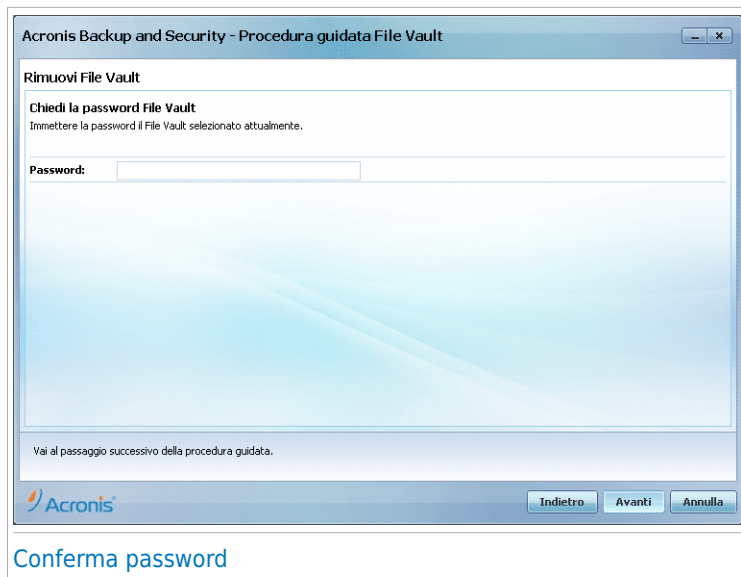
Se selezionate **Trovare un Vault File**, dovete cliccare su **Sfoglia** e selezionare il vault. Dovrete andare al passo 3 se il vault selezionato è aperto (montato) o al passo 2 se è bloccato (smontato).

Se cliccate su **Selezionare un Vault esistente**, dovrete poi cliccare sul nome del vault desiderato. Dovrete andare al passo 3 se il vault selezionato è aperto (montato) o al passo 2 se è bloccato (smontato).

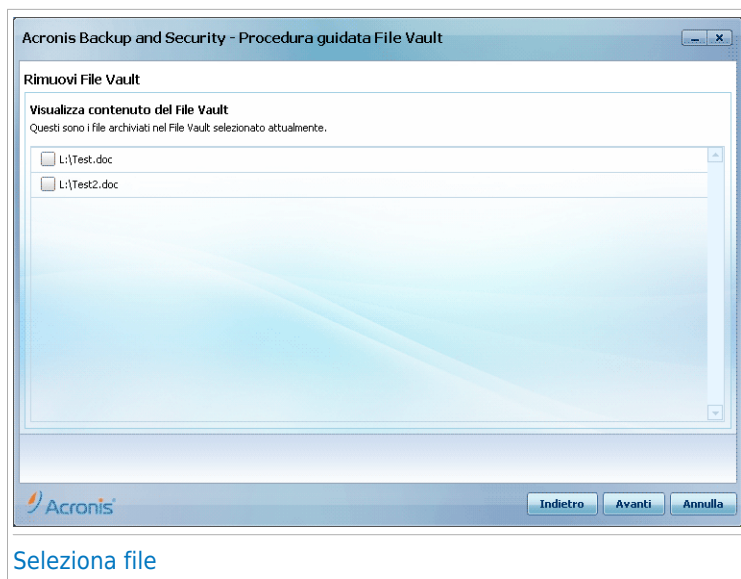
Selezionare **Avanti**.

Passo 2/5 - Password

Qui è dove vi verrà chiesto di inserire la password per il vault selezionato.

Conferma password

Digitare la password nel campo corrispondente e cliccare su **Avanti**.

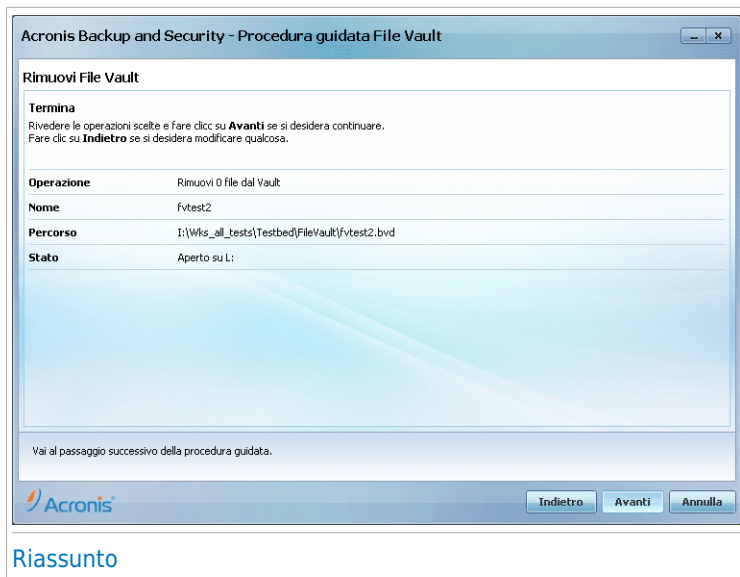
Passo 3/5 - Selezionare file

Qui è dove vi verrà chiesta la lista dei file del vault selezionato in precedenza.

Seleziona file

Selezionare i file da rimuovere e cliccare su **Avanti**.

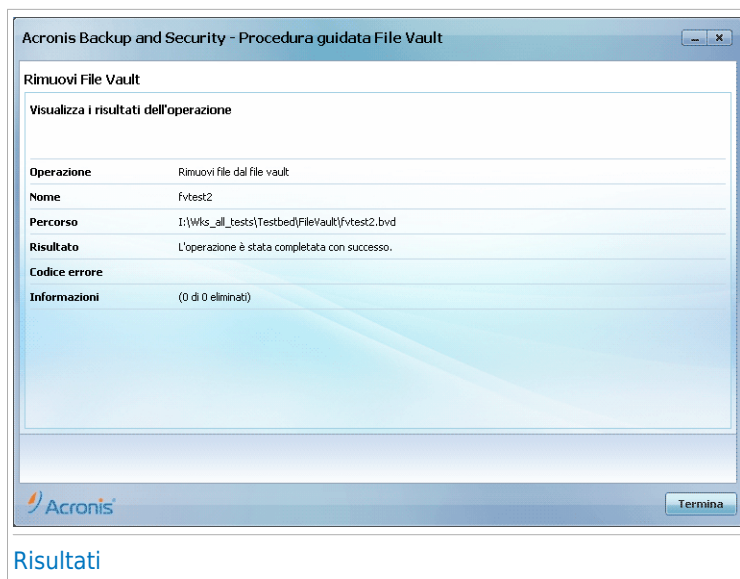
Passo 4/5 - Sommario

Qui è dove potrete rivedere le operazioni selezionate.

Riassunto

Selezionare **Avanti**.

Passo 5/5 – Risultati

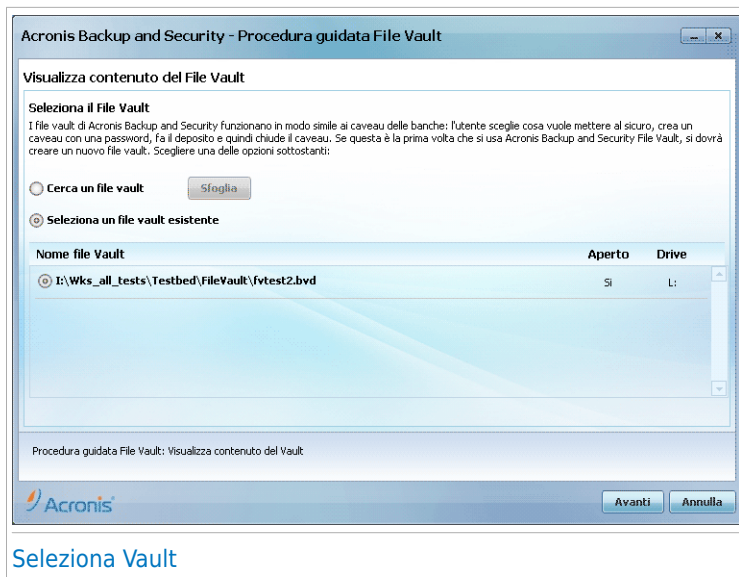
Qui potete vedere il risultato dell'operazione.

Risultati

Selezionare **Termina**.

10.4.3. Visualizza File Vault

Questo assistente permette di aprire uno specifico file vault e visualizzare i file al suo interno.

Passo 1/4 - Selezionare Vault

Qui potete specificare il vault dal quale visualizzare i file.

Seleziona Vault

Se selezionate **Trovare un Vault File**, dovete cliccare su **Sfoglia** e selezionare il vault. Dovrete andare al passo 3 se il vault selezionato è aperto (montato) o al passo 2 se è bloccato (smontato).

Se cliccate su **Selezionare un Vault esistente**, dovrete poi cliccare sul nome del vault desiderato. Dovrete andare al passo 3 se il vault selezionato è aperto (montato) o al passo 2 se è bloccato (smontato).

Selezionare **Avanti**.

Passo 2/4 - Password

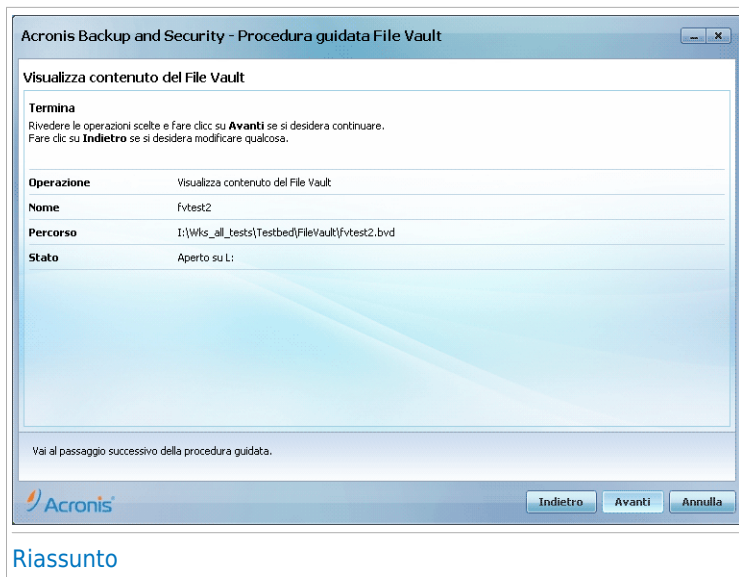
Qui è dove vi verrà chiesto di inserire la password per il vault selezionato.

Conferma password

Digitare la password nel campo corrispondente e cliccare su **Avanti**.

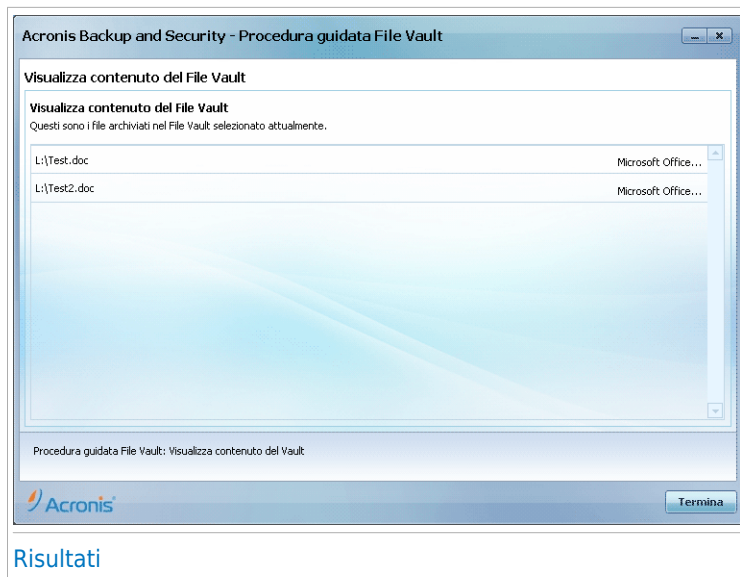
Passo 3/4 - Sommario

Qui è dove potrete rivedere le operazioni selezionate.

Riassunto

Selezionare **Avanti**.

Passo 4/4 – Risultati

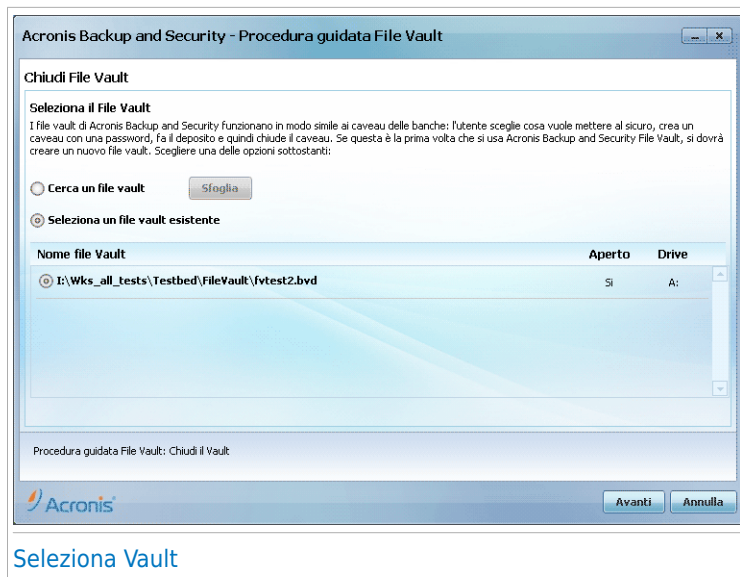
Qui è dove potete visualizzare i file del vault.

Risultati

Selezionare **Termina**.

10.4.4. Blocca File Vault

Questo assistente permette di bloccare uno specifico file vault per proteggere il suo contenuto.

Passo 1/3 - Selezionare Vault

Qui potete specificare il vault da bloccare.

Seleziona Vault

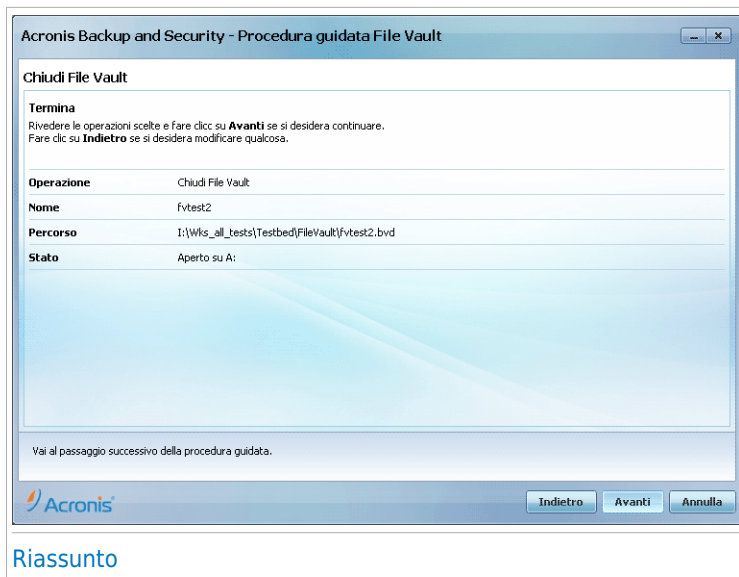
Se selezionate **Cercare un Vault File**, dovete cliccare su **Sfoglia** e selezionare il vault.

Se cliccate su **Selezionare un Vault File esistente** dovrete poi cliccare sul nome del vault desiderato.

Selezionare **Avanti**.

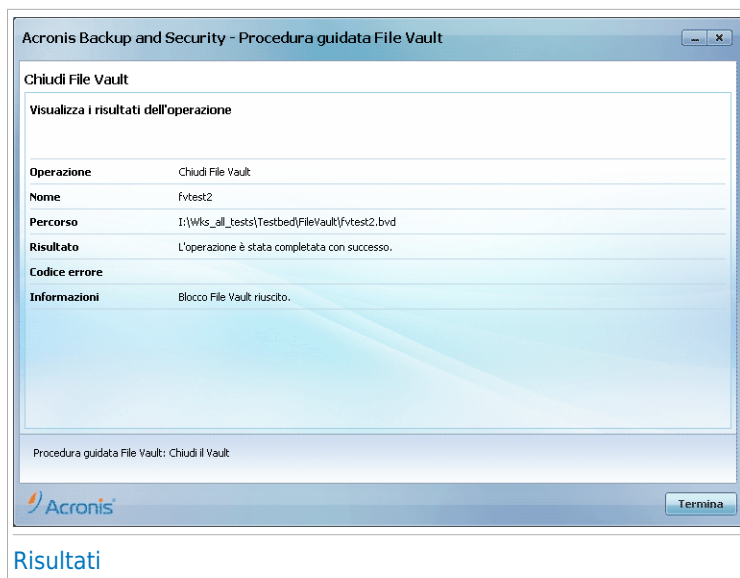
Passo 2/3 - Sommario

Qui è dove potrete rivedere le operazioni selezionate.

Riassunto

Selezionare **Avanti**.

Passo 3/3 – Risultati

Qui potete vedere il risultato dell'operazione.

Risultati

Selezionare **Termina**.

Modalità intermedia

11. Dashboard

La scheda Dashboard fornisce informazioni sullo stato di sicurezza del computer e permette di risolvere i problemi in sospeso.

Dashboard

La Dashboard è costituita dalle seguenti sezioni:

- **Stato Generale** - Indica il numero di problemi che influiscono sul computer ed aiuta a risolverli. Se vi sono problemi in sospeso verrà visualizzato un **cerchio rosso con un punto esclamativo** e il pulsante **Risolvi tutto**. Fare clic sul pulsante per avviare l'assistente Risolvi tutto.
- **Dettagli Stato** - Indica lo stato di ciascun modulo principale utilizzando frasi esplicite e una delle seguenti icone:

  Cerchio verde con un segno di spunta: Non vi sono problemi che influenzano lo stato di sicurezza. Il computer e i dati sono protetti.

  Cerchio grigio con un punto esclamativo: L'attività dei componenti di questo modulo non viene monitorata. Di conseguenza non vi sono informazioni disponibili sullo stato di sicurezza di tali componenti. Potrebbero esservi problemi specifici relativi a questo modulo.

  Cerchio rosso con un punto esclamativo: Vi sono problemi che influiscono sulla sicurezza del sistema. I problemi critici richiedono immediata attenzione. Anche i problemi non critici dovrebbero essere affrontati il più presto possibile.

Fare clic sul nome di un modulo per visualizzare ulteriori dettagli sul suo stato e per configurare il monitoraggio dello stato dei suoi componenti.

- **Profilo di Utilizzo** - Indica il profilo di utilizzo attualmente selezionato e offre link alle attività collegate a tale profilo:
  - Quando è selezionato il profilo **Tipico** il pulsante **Scansione Ora** permettere di compiere una scansione del sistema utilizzando l'Assistente Scansione Antivirus. Verrà esaminato l'intero sistema, con l'eccezione degli archivi. Nella configurazione di default, viene effettuata la scansione alla ricerca di tutti i tipi di malware eccettuati i rootkit.
  - Quando viene selezionato il profilo **Giocatore** il pulsante **Attiva/disattiva Modalità Gioco** permette di attivare/disattivare la Modalità Gioco. La Modalità Gioco modifica temporaneamente le impostazioni di protezione in modo di minimizzare l'impatto sulle prestazioni del sistema.
  - Quando è selezionato il profilo **Personalizzato** il pulsante **Aggiorna Ora** avvia un aggiornamento immediato. Apparirà una nuova finestra, dove potrete visualizzare lo stato dell'aggiornamento.

Se si desidera passare ad un profilo differente oppure modificare il profilo attualmente in uso, fare clic sul profilo e seguire l'assistente di configurazione.

12. Sicurezza

Acronis Backup and Security 2010 contiene un modulo di Sicurezza che vi aiuta a mantenere il vostro Acronis Backup and Security 2010 aggiornato ed il vostro computer libero di virus. Per accedere al modulo Sicurezza, cliccare sulla linguetta **Sicurezza**.

Sicurezza

Il modulo Sicurezza ha due sezioni:

- **Area di Stato** - Visualizza lo stato attuale di tutti i componenti di sicurezza monitorati e permette di selezionare quali componenti monitorare.
- **Attività Veloci** - Qui si trovano i collegamenti alle attività di sicurezza più importanti: aggiornamento immediato, scansione documenti, scansione del sistema, scansione appprofondita del sistema, scansione personalizzata e scansione vulnerabilità.

12.1. Area di Stato

L'area di stato è l'area in cui può essere visualizzato l'elenco completo dei componenti di sicurezza controllati e del loro stato attuale. Controllando ogni modulo di sicurezza Acronis Backup and Security 2010 informerà non solo quando vengono configurate impostazioni che possono influenzare la sicurezza del computer ma anche quando vengono dimenticate attività importanti.

Lo stato attuale di un componente è indicato utilizzando frasi esplicite e una delle icone seguenti:

Cerchio verde con un segno di spunta: Nessun problema riscontrato sul componente.

Cerchio rosso con un punto esclamativo: Alcuni problemi riscontrati sul componente.

Le frasi di descrizione dei problemi sono visualizzate in rosso. Fare clic sul pulsante **Risolvi** corrispondente ad una frase per risolvere il problema riportato. Se un problema non viene risolto subito seguire l'assistente per risolverlo.

12.1.1. Configurazione del Monitoraggio Stato

Per selezionare i componenti che Acronis Backup and Security 2010 deve monitorare, fare clic su **Configura Status Alerts** e selezionare la casella di controllo **Abilita avvisi** corrispondente alle caratteristiche che si desidera monitorare.

Importante

E' necessario abilitare il controllo dello stato di un componente se si desidera ricevere notifiche quando vi sono problemi che influenzano la sicurezza di tale componente. Per assicurarsi che il sistema sia completamente protetto abilitare il monitoraggio per tutti i componenti e risolvere tutti i problemi riportati.

Acronis Backup and Security 2010 può monitorare lo stato dei seguenti componenti di sicurezza:

- **Antivirus** - Acronis Backup and Security 2010 controlla lo stato dei due componenti della funzione Antivirus: protezione in tempo reale e scansione a richiesta. I problemi più comuni riportati per questo componente vengono elencati nella seguente tabella.

Problema	Descrizione
La protezione in tempo reale è disabilitata	I file non vengono controllati quando viene effettuato l'accesso da parte vostra o da parte di un'applicazione in esecuzione sul sistema.
Non è mai stata eseguita la scansione del computer alla ricerca di malware	Non è mai stata compiuta una scansione del sistema su richiesta per controllare che i file contenuti sul computer siano esenti da malware.
L'ultima scansione di sistema avviata è stata annullata prima della sua conclusione	È stata avviata, ma non completata, una scansione completa del sistema.

Problema	Descrizione
L'Antivirus è in uno stato critico	La protezione in tempo reale del sistema è disabilitata e la scansione del sistema è ormai necessaria da lungo tempo.

- **Aggiornamento** - Acronis Backup and Security 2010 controlla se le firme del malware sono aggiornate. I problemi più comuni riportati per questo componente vengono elencati nella seguente tabella.

Problema	Descrizione
L'Aggiornamento Automatico è disabilitato	Le firme del malware del prodotto Acronis Backup and Security 2010 non vengono aggiornate automaticamente e regolarmente.
L'aggiornamento non è stato compiuto per x giorni	Le firme del malware del prodotto Acronis Backup and Security 2010 sono obsolete.

- **Firewall** - Acronis Backup and Security 2010 controlla lo stato della funzione Firewall. Se non è abilitata, verra riportato il problema **Firewall disabilitato**.
- **Antispam** - Acronis Backup and Security 2010 controlla lo stato della funzione Antispam. Se non è abilitata, verra riportato il problema **Antispam disabilitato**.
- **Antiphishing** - Acronis Backup and Security 2010 controlla lo stato della funzione di Antiphishing. Se non è abilitata per tutte le applicazioni supportate, verrà riportato il problema **Antiphishing disabilitato**.
- **Controllo Vulnerabilità** - Acronis Backup and Security 2010 tiene traccia della funzione Controllo Vulnerabilità. Controllo Vulnerabilità comunica all'utente la necessità di installare aggiornamenti di Windows, aggiornamenti dell'applicazione e se è necessario rinforzare alcune password.

  I problemi più comuni riportati per questo componente vengono elencati nella seguente tabella.

Stato	Descrizione
Controllo Vulnerabilità è disabilitato	Acronis Backup and Security 2010 non controlla potenziali vulnerabilità relative ad aggiornamenti di Windows mancanti, aggiornamenti delle applicazioni o password deboli.

Stato	Descrizione
Sono state individuate molteplici vulnerabilità	Acronis Backup and Security 2010 ha trovato aggiornamenti di Windows/di applicazioni mancanti e/o password deboli.
Aggiornamenti critici Microsoft	Sono disponibili aggiornamenti di Windows critici, ma non sono stati installati.
Altri aggiornamenti Microsoft	Sono disponibili aggiornamenti di Windows non critici, ma non sono stati installati.
L'aggiornamento automatico di Windows è disabilitato	Gli aggiornamenti automatici di Windows non vengono automaticamente installati man mano che divengono disponibili.
Applicazione (obsoleta)	È disponibile una nuova versione dell'Applicazione ma non è stata installata.
Utente (Password Debole)	Individui malintenzionati possono individuare una password utente utilizzando software speciale.

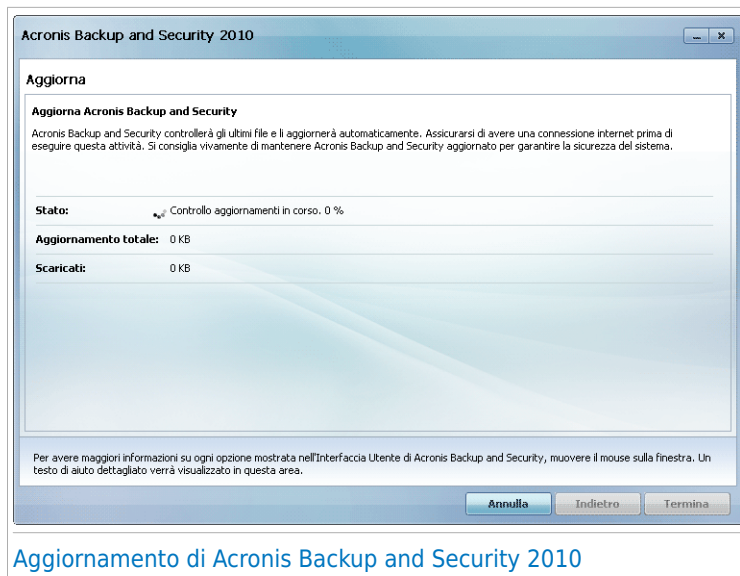
12.2. Funzioni Veloci

In questo elenco è possibile trovare dei link alle attività di sicurezza più importanti:

- **Aggiorna adesso** - inizia un aggiornamento immediato.
- **Scansione del Sistema** - avvia una scansione completa del computer (archivi esclusi). Per ulteriori attività di scansione a richiesta, fare clic su su questo pulsante e selezionare un'attività di scansione differente: Scansione Documenti o Scansione Approfondita del Sistema.
- **Scansione Personalizzata** - avvia un assistente che permette di creare ed eseguire un'attività di scansione personalizzata.
- **Scansione Vulnerabilità** - avvia una procedura guidata che controlla il sistema alla ricerca di vulnerabilità ed aiuta a risolverle.

12.2.1. Aggiornamento di Acronis Backup and Security 2010

Tutti giorni vengono trovati ed identificati nuovi malware. E' quindi molto importante mantenere aggiornato il vostro Acronis Backup and Security 2010 con le impronte più recenti del malware.

Di default, Acronis Backup and Security 2010 controlla se ci sono aggiornamenti quando accendete il computer ed in seguito **ogni ora**. Ad ogni modo, se si vuole aggiornare Acronis Backup and Security 2010, cliccare semplicemente su **Aggiorna adesso**. Il processo di aggiornamento verrà iniziato ed apparirà immediatamente la seguente finestra:

Aggiornamento di Acronis Backup and Security 2010

In questa finestra potete visualizzare lo stato del processo di aggiornamento.

Il processo di aggiornamento viene eseguito in volo, il chè vuol dire che i file da aggiornare vengono sostituiti progressivamente. In questo modo, il processo di aggiornamento non interesserà l'operatività del prodotto, nello stesso tempo, ogni vulnerabilità verrà esclusa.

Se si desidera chiudere questa finestra, cliccare semplicemente su **Annulla**. Ad ogni modo, questo non fermerà il processo di aggiornamento.

Nota

Se siete connessi a Internet mediante una connessione telefonica, è consigliato l'aggiornamento periodico di Acronis Backup and Security 2010 su richiesta dell'utente.

Riavviare il computer se richiesto. In caso di un aggiornamento importante, verrà chiesto di riavviare il computer. Cliccare su **Riavviare** per riavviare il sistema immediatamente.

Se si desidera riavviare il sistema più tardi, cliccare semplicemente su **OK**. Si consiglia di riavviare il sistema al più presto.

12.2.2. Scansione con Acronis Backup and Security 2010

Per avviare la scansione del vostro computer alla ricerca di malware, eseguire un task particolare di scansione facendo clic sul pulsante corrispondente o

selezionandolo dal menu a tendina. La seguente tabella elenca i task di scansione disponibili, assieme alla loro descrizione:

Task	Descrizione
Scansione sistema	Esamina l'intero sistema, esclusi gli archivi. Nella configurazione di default la scansione ricerca tutti i tipi di malware ad eccezione dei rootkit.
Scansione Documenti	Usare questa funzione per esaminare le cartelle importanti dell'utente corrente: `Documenti`, `Desktop` e `Avvio`. Questo garantirà la sicurezza dei vostri documenti, uno spazio di lavoro sicuro e l'esecuzione di applicazioni pulite all'avvio.
Scansione del Sistema approfondita	Esamina l'intero sistema. Nella configurazione predefinita, esegue la scansione per tutti i tipi di malware che minacciano la sicurezza del vostro sistema, come virus, spyware, adware, rootkits ed altri.
Personalizzare Scansione	Usare questa funzione per scegliere file e cartelle specifici da esaminare.

Nota

Poiché le funzioni **Scansione approfondita del sistema** e **Scansione completa del sistema** analizzano l'intero sistema, la scansione può richiedere un po' di tempo. Quindi consigliamo di eseguire questi compiti con priorità bassa o, meglio, quando il sistema è inattivo.

Quando si esegue una Scansione del Sistema, Scansione Approfondita del Sistema o Scansione Documenti, apparirà l'assistente Scansione Antivirus. Seguire la procedura di tre passi per completare il processo di scansione. Per ulteriori informazioni sulla procedura guidata, far riferimento a *«Procedura guidata scansione antivirus»* (p. 46).

Quando si esegue una Scansione Personalizzata, l'assistente Scansione Personalizzata vi condurrà lungo il processo di scansione. Seguire i sei passi della procedura guidata per effettuare la scansione di file o cartelle specifiche. Per ulteriori informazioni sulla procedura guidata, far riferimento a *«Assistente Scansione Personalizzata»* (p. 51).

12.2.3. Ricerca delle Vulnerabilità

La Scansione delle Vulnerabilità controlla gli Aggiornamenti di Microsoft Windows, di Microsoft Windows Office e le password dei tuoi account di Microsoft Windows per assicurare che il tuo Sistema Operativo sia aggiornato e che le password non siano vulnerabili.

Per controllare il vostro computer alla ricerca di vulnerabilità, cliccare su **Scansione Vulnerabilità** e seguire i sei passi della procedura guidata. Per ulteriori informazioni fare riferimento a *«Correggi Vulnerabilità»* (p. 235).

13. Genitori

Acronis Backup and Security 2010 include un modulo Controllo genitori. Il Controllo genitori consente di restringere l'accesso a Internet e a applicazioni specifiche da parte dei figli. Per controllare lo stato del Controllo Genitori, fare clic sulla scheda **Genitori**.

Genitori

Il modulo Genitori ha due sezioni:

- **Area di Stato** - Permette di verificare se il Controllo Genitori è configurato e di abilitare/disabilitare il controllo dell'attività di tale modulo.
- **Attività Veloci** - Qui si trovano i link alle attività di sicurezza più importanti: scansione del sistema, scansione approfondita del sistema e aggiornamento immediato.

13.1. Area di Stato

Lo stato attuale del modulo Controllo Genitori è indicato utilizzando frasi esplicite e una delle icone seguenti:

Cerchio verde con un segno di spunta: Nessun problema riscontrato sul componente.

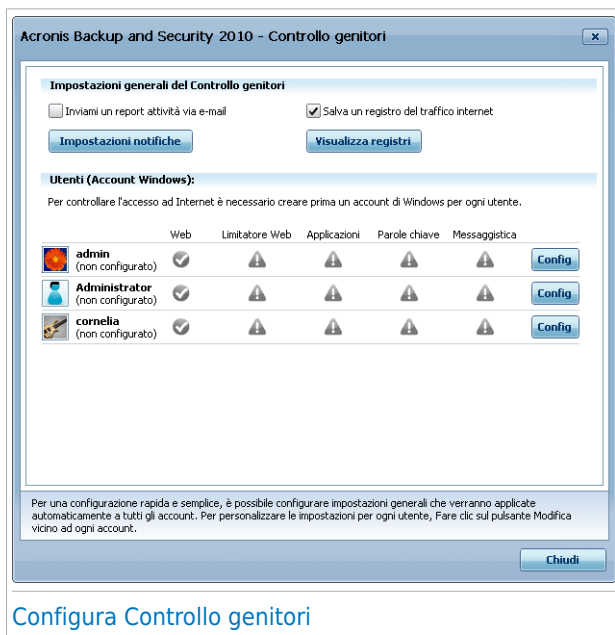
Cerchio rosso con un punto esclamativo: Alcuni problemi riscontrati sul componente.

Le frasi di descrizione dei problemi sono visualizzate in rosso. Fare clic sul pulsante **Risolvi** corrispondente ad una frase per risolvere il problema riportato. Il problema più comune riportato per questo modulo è **Controllo Genitori non configurato**.

Se si desidera che Acronis Backup and Security 2010 controlli il modulo Controllo Genitori fare clic su **Configura Status Alerts** e selezionare la casella di controllo **Abilita avvisi** per questo modulo.

13.2. Funzioni Veloci

Per configurare il Controllo Genitori, fare clic su **Controllo Genitori** nell'area Funzioni Veloci. Apparirà una nuova finestra.

Configura Controllo genitori

Qui è possibile vedere lo stato del Controllo Genitori per ogni account utente di Windows ed è possibile configurare le regole del Controllo Genitori. Questa finestra di configurazione è simile alla scheda Controllo Genitori in Modalità Avanzata. Per ulteriori informazioni fare riferimento a *«Controllo genitori»* (p. 176).

14. File Vault

Acronis Backup and Security 2010 contiene un modulo File Vault che permette di mantenere i dati, non solo sicuri, ma anche confidenziali. Per conseguire questo obiettivo, utilizzare la criptazione dei file.

Per accedere al modulo File Vault, fare clic sulla scheda **File Vault**.

File Vault

Il modulo File Vault contiene due sezioni:

- **Area di Stato** - Permette di visualizzare l'elenco completo dei componenti monitorati. È possibile scegliere quali componenti monitorare. Si consiglia di abilitare l'opzione di monitoraggio per tutti i componenti.
- **Attività Veloci** - Qui si trovano i link alle più importanti funzioni di sicurezza: aggiunta, visualizzazione e rimozione dei file vault.

14.1. Area di Stato

Lo stato attuale di un componente è indicato utilizzando frasi esplicite e una delle icone seguenti:

Cerchio verde con un segno di spunta: Nessun problema riscontrato sul componente.

Cerchio rosso con un punto esclamativo: Alcuni problemi riscontrati sul componente.

Le frasi di descrizione dei problemi sono visualizzate in rosso. Fare clic sul pulsante **Risolvi** corrispondente ad una frase per risolvere il problema riportato. Se un problema non viene risolto subito seguire l'assistente per risolverlo.

L'area di stato della scheda File Vault fornisce informazioni sullo stato del modulo **Criptazione File**.

Se si desidera che Acronis Backup and Security 2010 controlli il modulo Criptazione File fare clic su **Configura Status Alerts** e selezionare la casella di controllo **Abilita avvisi**.

14.2. Funzioni Veloci

Sono disponibili i seguenti tasti:

- **Aggiungere File alla Criptazione** - inizia la procedura guidata che vi permette di immagazzinare i vostri file / documenti importanti privatamente mediante la loro criptazione in speciali drive protetti. Per ulteriori informazioni fare riferimento a *«Aggiungi file alla Criptazione (Vault)»* (p. 65).
- **Rimuovere File dalla Criptazione** - inizia la procedura guidata che vi permette di cancellare dati dai file prottetti. Per ulteriori informazioni fare riferimento a *«Rimuovi Vault File»* (p. 71).
- **Visualizzare File Vault** - inizia la procedura guidata che vi permette di visualizzare il contenuto dei file vault. Per ulteriori informazioni fare riferimento a *«Visualizza File Vault»* (p. 76).
- **Bloccare File Vault** - inizia la procedura guidata che permette di bloccare un file vault per iniziare a proteggere il suo contenuto. Per ulteriori informazioni fare riferimento a *«Blocca File Vault»* (p. 80).

15. Rete

Il modulo Rete vi permette gestire i prodotti Acronis installati sui computer di casa da un singolo computer. Per accedere al modulo Rete, fare clic sulla scheda **Rete**.

Importante

Può gestire solo i seguenti prodotti di sicurezza Acronis:

- Acronis AntiVirus 2010
- Acronis Internet Security Suite 2010
- Acronis Backup and Security 2010

Rete

Per essere in grado di gestire i prodotti Acronis installati sui computer di casa, dovete seguire questi passaggi:

1. Unirvi alla rete domestica Acronis sul vostro computer. Unirsi alla rete consiste in configurare una password di amministrazione per la gestione della rete domestica.
2. Andare su ogni computer che si vuole gestire ed aggiungerli alla rete (impostare la password).
3. Tornare al vostro computer ed aggiungere i computer che volete gestire.

15.1. Funzioni Veloci

Inizialmente, solo un tasto sarà disponibile.

- **Abilita Rete** - permette di impostare una password di rete, pertanto creando e accedendo ad una rete.

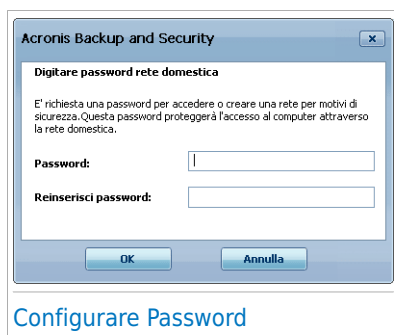
Dopo aversi unito alla rete, appariranno molti più tasti.

- **Disabilita Rete** - permette di lasciare la rete.
- **Aggiungi Computer** - permette di aggiungere computer alla rete.
- **Esaminare Tutti** - vi permette di eseguire la scansione su tutti i computer in gestione contemporaneamente.
- **Aggiornare Tutti** vi permette di aggiornare tutti i computer in gestione contemporaneamente.

15.1.1. Unirsi alla Rete Acronis

Per unirsi alla rete domestica Acronis, seguire questi passaggi:

1. Fare clic su **Abilita rete**. Vi verrà chiesto di configurare le password per la gestione domestica.

Configurare Password

2. Inserire la stessa password in ognuno dei campi corrispondenti.
3. Selezionare **OK**.

Potete vedere il nome del computer apparire nella mappa della rete.

15.1.2. Aggiungere dei computer alla Rete Acronis

Prima di poter aggiungere un computer alla rete domestica Acronis dovrete configurare la password per la gestione domestica Acronis sul rispettivo computer.

Per aggiungere un computer alla rete domestica Acronis , seguire questi passi:

1. Fare clic su **Aggiungi Computer**. Vi verrà chiesto di fornire la password per la gestione domestica locale.

Inserire Password

2. Digitare la password per la gestione domestica e cliccare su **OK**. Apparirà una nuova finestra.

Aggiungi Computer

Potete vedere l'elenco dei computer in questa rete. Il significato dell'icona è il seguente:

Indica un computer online senza prodotti Acronis gestibile installati.

Indica un computer online con un prodotto di Acronis gestibile installato.

Indica un computer offline con un prodotto di Acronis gestibile installato.

3. Eseguire una delle seguenti azioni:
   - Selezionare dall'elenco il nome del computer da aggiungere.
   - Digitare l'indirizzo IP o il nome del computer da aggiungere nel campo corrispondente.

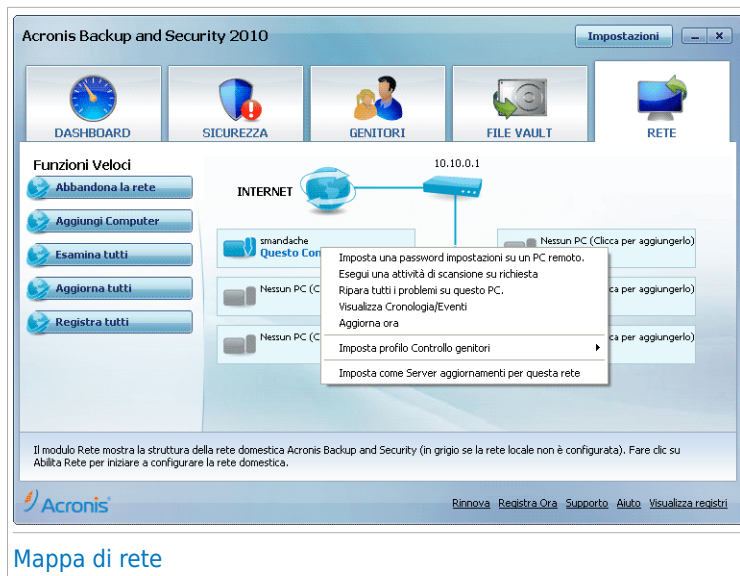
4. Selezionare **Aggiungi**. Vi verrà chiesto di fornire la password per la gestione domestica sul rispettivo computer.

Autenticare

5. Digitare la password per la gestione domestica configurata sul rispettivo computer.
6. Selezionare **OK**. Se avete fornito la password corretta, il nome del computer selezionato apparirà nella mappa di rete.

Nota
Potete aggiungere fino a cinque computer alla mappa di rete.

15.1.3. Gestione della Rete Acronis

Una volta che avete creato con successo una rete domestica Acronis, potrete gestire tutti i prodotti Acronis da un singolo computer.

Mappa di rete

Se muovete il cursore su un computer nella mappa di rete, potete vedere una breve informazione su di esso (nome, indirizzo IP, numero di problemi che colpiscono la sicureza del sistema).

Se si fa clic con il pulsante destro sul nome del computer nella mappa di rete, è possibile vedere tutte le funzioni di amministrazione che si possono eseguire dal computer remoto.

- **Rimuovi il PC dalla rete domestica**

  Permette di rimuovere il PC dalla rete.

- **Stabilire una password per le impostazioni su un PC remoto**

  Permette di creare una password per limitare l'accesso alle impostazioni Acronis sul PC.

- **Eseguire una attività di scansione su richiesta**

  Permette di eseguire una scansione a richiesta sul computer remoto. E' possibile compiere una qualsiasi delle seguenti attività di scansione: Scansione Documenti, Scansione del Sistema o Scansione del Sistema Approfondita.

- **Risolvere tutti i problemi su questo computer**

  Permette di risolvere i problemi che influenzano la sicurezza del computer seguendo l'assistente Risolvi tutto.

- **Visualizzare Cronologia/Eventi**

Permette di accedere al modulo **Cronologia&Eventi** del prodotto Acronis installato sul computer.

- **Aggiorna adesso**

  Avvia il processo di aggiornamento per il prodotto Acronis installato sul computer.

- **Imposta Profilo Controllo genitori**

  Permette di impostare la categoria di età da utilizzare per il filtro web del Controllo Genitori del computer: bambino, adolescente o adulto.

- **Impostare come Server di aggiornamento per questa rete**

  Permette di impostare il computer come server di aggiornamento per tutti i prodotti Acronis installati sui computer della rete. Utilizzando questa opzione si ridurrà il traffico Internet, poiché un solo computer della rete si collegherà ad Internet per scaricare gli aggiornamenti.

Prima di eseguire una funzione su un particolare computer, vi verrà chiesto di fornire la password per la gestione domestica locale.

Inserire Password

Digitare la password per la gestione domestica e cliccare su **OK**.

Nota

Se si ha in programma di eseguire diverse funzioni, è possibile selezionare **Non mostrare di nuovo questo messaggio durante questa sessione**. Selezionando questa opzione non vi verrà più chiesta la password durante la sessione corrente.

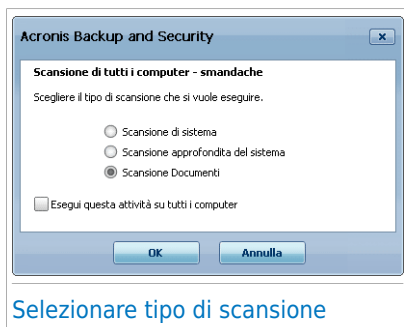
15.1.4. Scansione di tutti i computer

Per esaminare tutti i computer in gestione, seguire questi passaggi:

1. Cliccare su **Esaminare Tutti**. Vi verrà chiesto di fornire la password per la gestione domestica locale.

Inserire Password

2. Selezionare un tipo di scansione.
   - **Scansione del Sistema** - inizia una scansione completa del computer (archivi esclusi).
   - **Scansione Approfondita del Sistema** - inizia una scansione completa del computer (archivi inclusi).
   - **Scansione Documenti** - inizia una scansione veloce dei documenti e delle impostazioni.

Selezionare tipo di scansione

3. Selezionare **OK**.

15.1.5. Aggiornamento di tutti i Computer

Per aggiornare tutti i computer in gestione, seguire questi passaggi:

1. Cliccare su **Aggiornare Tutti**. Vi verrà chiesto di fornire la password per la gestione domestica locale.

Inserire Password

2. Selezionare **OK**.

Modalità avanzata

16. Generale

Il modulo Generale fornisce informazioni sull'attività di Acronis Backup and Security 2010 e sul sistema. Qui potete anche modificare il comportamento generale di Acronis Backup and Security 2010.

16.1. Dashboard

Per visualizzare le statistiche di attività del prodotto, lo stato di registrazione e se vi sono problemi che influiscono sul computer, andare a **Generale>Dashboard** in Modalità Avanzata.

Dashboard

La Dashboard ha diverse sezioni:

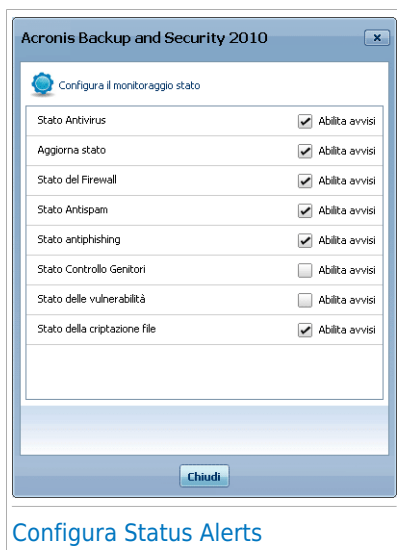
- **Stato Generale** - Informa in merito a qualsiasi problema che influenza la sicurezza del computer.
- **Statistiche** - Mostra importanti informazioni riguardanti l'attività di Acronis Backup and Security 2010.
- **Informazioni generali** - Mostra lo stato dell'aggiornamento, della registrazione ed informazioni sulla licenza.

- **Attività file** - Indica l'evoluzione del numero di elementi esaminati dall'Antimalware di Acronis Backup and Security 2010. L'altezza della barra indica l'intensità del traffico durante un intervallo di tempo.
- **Attività rete** - Indica l'evoluzione del traffico di rete filtrato dal Firewall Acronis Backup and Security 2010. L'altezza della barra indica l'intensità del traffico durante quell'intervallo di tempo.

16.1.1. Stato generale

Qui è possibile trovare il numero di problemi che mettono a rischio la sicurezza del computer. Per rimuovere tutte le minacce, fare clic su **Risolvi tutto**. Questo riavvia la procedura guidata Risolvi tutto.

Per configurare quali moduli verranno monitorati da Acronis Backup and Security 2010, fare clic su **Configura Status Alerts**. Apparirà una nuova finestra:

Configura Status Alerts

Se si desidera che Acronis Backup and Security 2010 monitori un componente, selezionare la casella di controllo **Abilita allarmi** per il componente corrispondente. Acronis Backup and Security 2010 può monitorare lo stato dei seguenti componenti di sicurezza:

- **Antivirus** - Acronis Backup and Security 2010 monitora lo stato dei due componenti della funzione Antivirus: protezione in tempo reale e scansione su richiesta. I problemi più comuni riportati per questo componente vengono elencati nella seguente tabella.

Problema	Descrizione
La protezione in tempo reale è disabilitata	I file non vengono controllati quando viene effettuato l'accesso da parte vostra o da parte di un'applicazione in esecuzione sul sistema.
Non è mai stata eseguita la scansione del computer alla ricerca di malware	Non è mai stata compiuta una scansione del sistema su richiesta per controllare che i file contenuti sul computer siano esenti da malware.
L'ultima scansione di sistema avviata è stata annullata prima della sua conclusione	È stata avviata, ma non completata, una scansione completa del sistema.
L'Antivirus è in uno stato critico	La protezione in tempo reale del sistema è disabilitata e la scansione del sistema è ormai necessaria da lungo tempo.

- **Aggiornamento** - Acronis Backup and Security 2010 controlla se le firme del malware sono aggiornate. I problemi più comuni riportati per questo componente vengono elencati nella seguente tabella.

Problema	Descrizione
L'Aggiornamento Automatico è disabilitato	Le firme del malware del prodotto Acronis Backup and Security 2010 non vengono aggiornate automaticamente e regolarmente.
L'aggiornamento non è stato compiuto per x giorni	Le firme del malware del prodotto Acronis Backup and Security 2010 sono obsolete.

- **Firewall** - Acronis Backup and Security 2010 controlla lo stato della funzione Firewall. Se non è abilitata, verra riportato il problema **Firewall disabilitato**.
- **Antispam** - Acronis Backup and Security 2010 controlla lo stato della funzione Antispam. Se non è abilitata, verra riportato il problema **Antispam disabilitato**.
- **Antiphishing** - Acronis Backup and Security 2010 controlla lo stato della funzione di Antiphishing. Se non è abilitata per tutte le applicazioni supportate, verrà riportato il problema **Antiphishing disabilitato**.
- **Controllo Genitori** - Acronis Backup and Security 2010 controlla lo stato della funzione Controllo Genitori. Se non è abilitata, verra riportato il problema **Controllo Genitori non configurato**.

- **Controllo Vulnerabilità** - Acronis Backup and Security 2010 tiene traccia della funzione Controllo Vulnerabilità. Controllo Vulnerabilità comunica all'utente la necessità di installare aggiornamenti di Windows, aggiornamenti dell'applicazione e se è necessario rinforzare alcune password.

  I problemi più comuni riportati per questo componente vengono elencati nella seguente tabella.

Stato	Descrizione
Controllo Vulnerabilità è disabilitato	Acronis Backup and Security 2010 non controlla potenziali vulnerabilità relative ad aggiornamenti di Windows mancanti, aggiornamenti delle applicazioni o password deboli.
Sono state individuate molteplici vulnerabilità	Acronis Backup and Security 2010 ha trovato aggiornamenti di Windows/di applicazioni mancanti e/o password deboli.
Aggiornamenti critici Microsoft	Sono disponibili aggiornamenti di Windows critici, ma non sono stati installati.
Altri aggiornamenti Microsoft	Sono disponibili aggiornamenti di Windows non critici, ma non sono stati installati.
L'aggiornamento automatico di Windows è disabilitato	Gli aggiornamenti automatici di Windows non vengono automaticamente installati man mano che divengono disponibili.
Applicazione (obsoleta)	È disponibile una nuova versione dell'Applicazione ma non è stata installata.
Utente (Password Debole)	Individui malintenzionati possono individuare una password utente utilizzando software speciale.

- **Criptazione File** controlla lo stato del File Vault. Se non è abilitata, verrà riportato il problema **Criptazione File disabilitata**.

Importante

Per assicurarsi che il sistema sia completamente protetto abilitare il monitoraggio per tutti i componenti e risolvere tutti i problemi riportati.

16.1.2. Statistiche

Se volete dare un'occhiata all'attività di Acronis Backup and Security 2010, un buon posto per cominciare è la sezione Statistiche. Potete visualizzare i seguenti elementi:

Elemento	Descrizione
File esaminati	Indica il numero di file che sono stati esaminati alla ricerca di malware al momento dell'ultima scansione.
File disinfettati	Indica il numero dei file che sono stati disinfettati al momento della vostra ultima scansione.
File infettati rilevati	Indica il numero di file infetti che sono stati trovati nel sistema al momento dell'ultima scansione.
Ultima scansione del sistema	Indicata l'ultima scansione del computer. Se l'ultima scansione è stata eseguita più di una settimana fa, eseguire al più presto una nuova scansione. Per eseguire una scansione di tutto il computer, fare clic sulla scheda **Antivirus**, Scansione virus, ed eseguire una Scansione completa di sistema o una Scansione approfondita di sistema.
Prossima scansione	Indica la prossima volta in cui il computer verrà sottoposto a scansione.

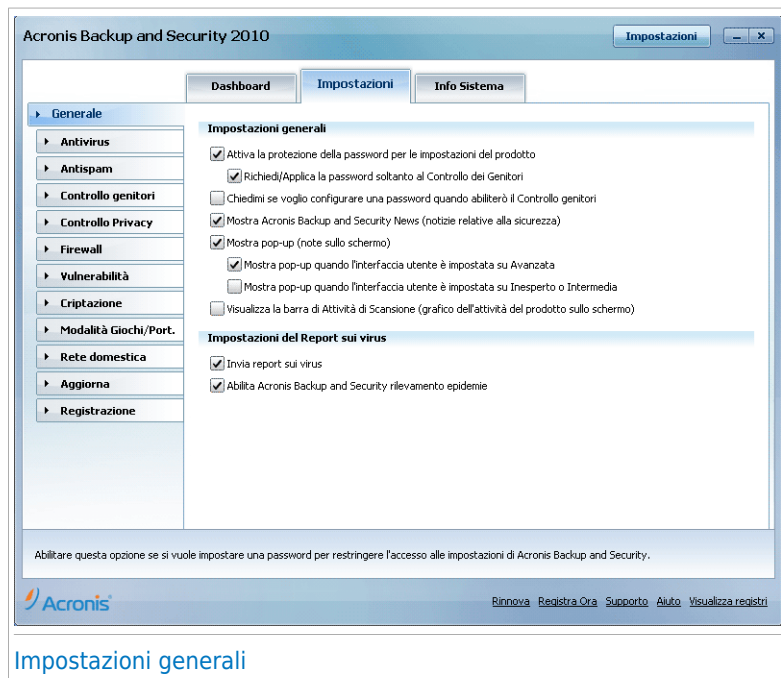
16.1.3. Panoramica

Qui è possibile vedere lo stato di aggiornamento e le informazioni sulla registrazione e la licenza.

Elemento	Descrizione
Ultimo aggiornamento	Indicata quando è stato aggiornato per l'ultima volta il prodotto Acronis Backup and Security 2010. Eseguire aggiornamenti regolari per avere un sistema completamente protetto.
Registrazione	Indica il tipo e lo stato della vostra chiave di licenza. Per mantenere sicuro il vostro sistema dovete rinnovare o aggiornare Acronis Backup and Security 2010 se la vostra chiave è scaduta.
Scade in	Indica il numero di giorni che mancano alla scadenza della chiave di licenza. Sa la chiave di licenza scade entro qualche giorno, registrare il prodotto con una nuova chiave di licenza. Per acquistare una chiave di licenza o rinnovare la licenza, fare clic sul link **Acquista/Rinnova**, situato in basso nella finestra.

16.2. Impostazioni

Per configurare e gestire le impostazioni generali di Acronis Backup and Security 2010 andare su **Generale>Impostazioni** in Modalità Avanzata.

Impostazioni generali

Da qui è possibile impostare il comportamento generale di Acronis Backup and Security 2010. Acronis Backup and Security 2010 è caricato automaticamente all'avvio di Windows e successivamente minimizzato nella barra strumenti.

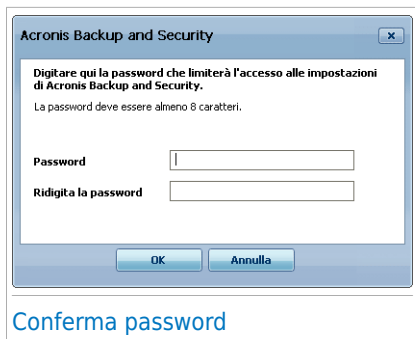
16.2.1. Impostazioni generali

- **Abilita la protezione password per le impostazioni del prodotto** - consente l'impostazione di una password per proteggere la configurazione di Acronis Backup and Security 2010.

Nota

Se non siete l'unica persona ad utilizzare questo computer, consigliamo di proteggere le vostre impostazioni di Acronis Backup and Security 2010 con una password.

Selezionando questa opzione, apparirà la seguente finestra:

Conferma password

Digitare la password nel campo **Password**, quindi re-inserirla nel campo **Ridigitare password** e selezionare **OK**.

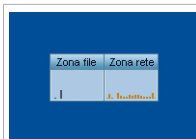
Una volta che avete impostato la password, vi verrà chiesta ogni volta che vorrete cambiare le impostazioni di Acronis Backup and Security 2010. Gli altri amministratori del sistema (se ci sono) dovranno anche loro fornire questapassword per cambiare le impostazioni di Acronis Backup and Security 2010.

Se volete che vi venga richiesta la password solo quando configurate il Controllo dei Genitori, dovrete selezionare anche **Chiedere/Applicare password al Controllo dei Genitori**. Inoltre, se una password è stata impostata per il Controllo dei Genitori e deselezionate questa opzione, la rispettiva password verrà chiesta per configurare qualsiasi opzione di Acronis Backup and Security 2010.

Importante

Se si dimentica la password, si deve riparare il prodotto per modificare la configurazione Acronis Backup and Security 2010.

- **Chiedimi se voglio configurare una password per l'abilitazione del Controllo dei Genitori** - vi chiede di configurare una password quando desiderate abilitare il Controllo dei Genitori e non è stata impostata nessuna. Impostando una password, impedirete ad altri utenti con diritti di amministratore di modificare le impostazioni del Controllo dei Genitori che avete configurato per un utente specifico.
- **Mostra Acronis Backup and Security News (notizie relative alla sicurezza)** - riceve di volta in volta, dai server Acronis, segnalazioni di sicurezza relative alla diffusione di nuovi virus.
- **Mostra pop-ups (attiva la schermata delle note)** - mostra finestre a tendina relative allo stato del prodotto. È possibile configurare Acronis Backup and Security 2010 affinché visualizzi pop-up solo quando l'interfaccia è nella Modalità Inesperto / Intermedia o nella Modalità Avanzata.

- **Vusalizza barra di attività della scansione (grafico dell'attività del prodotto a schermo)** - mostra la barra delle Attività della Scansione ogni volta che si accede a Windows. Deselezionare la casella se non volete che la barra delle Attività di Scansione venga mostrata ancora.

Barra di Attività della Scansione

Nota

Questa opzione può essere configurata solo per l'account di Windows in uso. La barra dell'attività di scansione è disponibile solo quando l'interfaccia è in Modalità Avanzata.

16.2.2. Impostazioni del Report sui virus

- **Invia rapporti dei virus** - invia ai Laboratori Acronis i rapporti relativi ai virus identificati sul vostro computer. Questo ci aiuta a tracciare la diffusione dei virus.

  I rapporti non contengono dati confidenziali, come il vostro nome, l'indirizzo IP o altri, e non verranno utilizzati per scopi commerciali. Le informazioni fornite conterranno solo il nome del virus e verranno utilizzate unicamente per creare rapporti statistici.

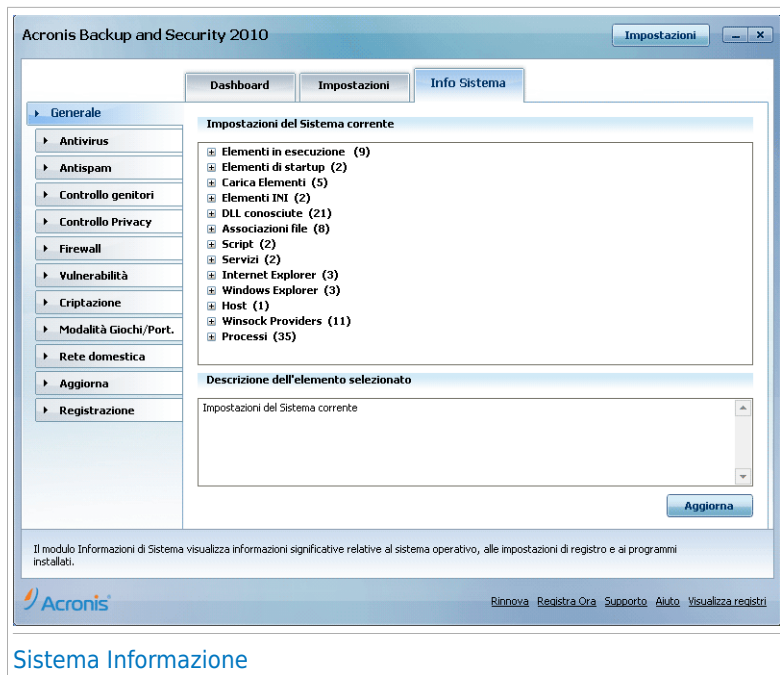
- **Attivare Outbreak Detection Acronis Backup and Security** - invia ai Laboratori Acronis i report relativi al potenziale scoppio di un virus.

  I report non contengono dati confidenziali, come il vostro nome, l'indirizzo IP o altri, e non verranno utilizzati per scopi commerciali. Le informazioni fornite conterranno esclusivamente il nome del virus e verranno utilizzate per creare report statistici.

16.3. Sistema Informazione

Acronis Backup and Security 2010 vi permette di visualizzare, da una singola ubicazione, tutta la configurazione del sistema e le applicazioni che verranno eseguite all'avvio. In questo modo potrete monitorare l'attività del sistema e delle applicazioni installate così come identificare possibili infezioni del sistema.

Per ottenere informazioni sul sistema, cliccare su **Generale>Informazioni di Sistema** in Modalità Avanzata.

Sistema Informazione

La lista contiene tutti gli elementi caricati quando si avvia il sistema oltre agli elementi caricati da varie applicazioni.

Tre pulsanti sono disponibili:

- **Ripristinare** - Cambia l'associazione di un file corrente a quella di default. Disponibile solo per le impostazioni delle **Associazioni File**!
- **Vai a** - apri una finestra dove l'elemento selezionato è situato (la **Registrazione** ad esempio).

Nota

A seconda dell'elemento selezionato, il pulsante **Vai a** potrebbe non apparire.

- **Aggiorna** - riapri la sezione del **Sistema Informazione** section.

17. Antivirus

Acronis Backup and Security 2010 protegge il vostro computer da ogni tipo di minaccia malware (virus, troiani, spyware, rootkit ed altro). La protezione che Acronis Backup and Security 2010 vi offre è divisa in due categorie:

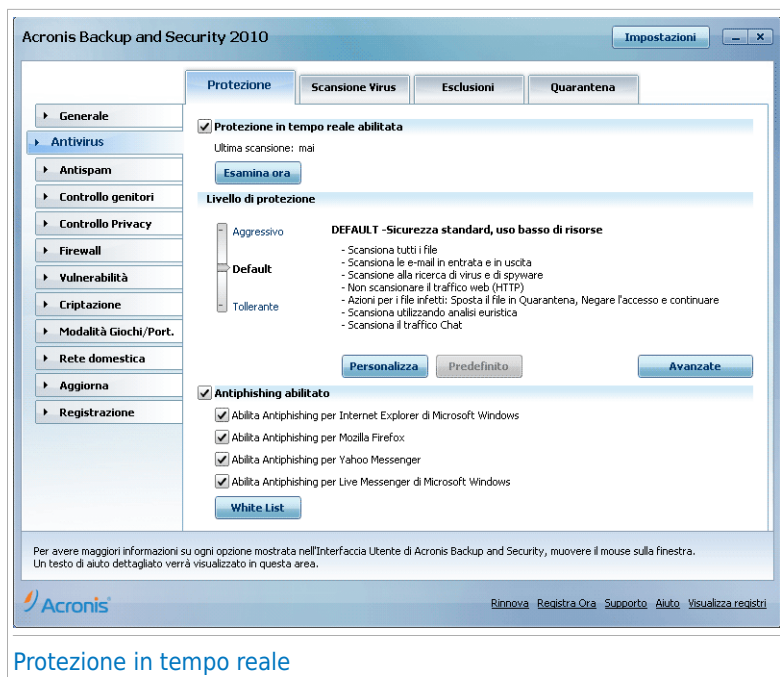
- Protezione in tempo reale - previene l'ingresso di nuove minacce malware nel vostro sistema. Acronis Backup and Security 2010 esaminerà, ad esempio, un documento word quando verrà aperto, ed una mail quando verrà ricevuta.

Nota
La protezione in tempo reale si riferisce anche alla scansione "all'accesso" - i file vengono esaminati nel momento in cui gli utenti vi accedono.

- Scansione a richiesta - permette di rilevare e di rimuovere malware già residente nel vostro sistema. Si tratta della classica scansione dei virus avviata dall'utente – si sceglie quale drive, cartella o file Acronis Backup and Security 2010 deve esaminare e Acronis Backup and Security 2010 li esamina – a richiesta. I processi della scansione vi permettono di creare routine di scansione personalizzate e la loro esecuzione può essere programmata con una cadenza regolare.

17.1. Protezione in tempo reale

Acronis Backup and Security 2010 fornisce una continua protezione in tempo reale contro un ampio spettro di minacce malware mediante la scansione di tutti i file nei quali si è effettuato l'accesso, le mail e le comunicazioni tramite applicazioni Software di Messaggistica Istantanea (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Acronis Backup and Security 2010 Antiphishing vi impedisce di svelare informazioni personali mentre navigate su internet avvertendovi delle potenziali pagine web con phishing.

Per configurare la protezione in tempo reale e la protezione Antiphishing, fare clic su **Antivirus>Shield** in Modalità Avanzata.

Protezione in tempo reale

Potete vedere se la Protezione in tempo reale è abilitata o disabilitata. Se volete cambiare lo stato della Protezione in tempo reale, selezionare o deselezionare la casella corrispondente.

Importante

Per impedire ai virus di infettare il vostro computer, tenere abilitato il **Virus Shield**.

Per avviare una scansione del sistema, fare clic su **Scansiona Ora**.

17.1.1. Configurazione del Livello di Protezione

Potete scegliere il livello di protezione che meglio si adatta alle vostre necessità di sicurezza. Trascinate il pulsante sulla barra per impostare il livello di protezione appropriato.

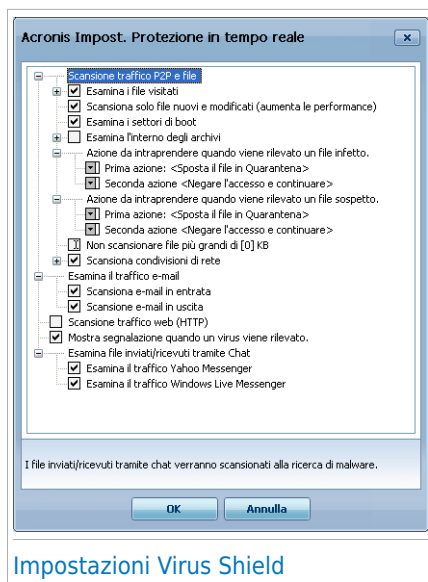
Ci sono 3 livelli di protezione:

Livello di protezione	Descrizione
Permissiva	Copre le necessità di sicurezza di base. Il livello di consumo delle risorse è molto basso. Solo i programmi e i messaggi di posta in arrivo sono scansionati solo alla ricerca di virus. Oltre alla classica scansione basata sulla firma, è utilizzata anche l'analisi euristica. Le azioni prese sui file infetti sono le seguenti: pulisci file/sposta in quarantena.
Default	Offre una sicureza standard. Il livello di consumo delle risorse è basso. Tutti i file e i messaggi di posta in arrivo ed in uscita sono esaminati alla ricerca di virus e spyware. Oltre alla classica scansione basata sull'impronta, è utilizzata anche l'analisi euristica. Le azioni prese sui file infetti sono le seguenti: pulisci file/sposta in quarantena.
Aggressiva	Offre una sicurezza alta. Il livello di consumo delle risorse è moderato. Tutti i file, e i messaggi e-mail in entrata ed in uscita ed il traffico web sono esaminati alla ricerca di virus e spyware. Oltre alla classica scansione basata sull'impronta, è utilizzata anche l'analisi euristica. Le azioni prese sui file infetti sono le seguenti: pulisci file/sposta in quarantena.

Per applicare le impostazioni di protezione in tempo reale di default cliccare su **Livello di Default**.

17.1.2. Livello di Protezione Personalizzato

Gli utenti esperti possono trarre vantaggio dalle possibilità di impostazione della scansione Acronis Backup and Security 2010. Infatti la scansione può essere impostata in modo di esaminare solo delle specifiche estensioni, di cercare delle particolare minacce malware, o di non esaminare gli archivi. Questo può ridurre di molto i tempi di scansione ed incrementare la reattività del vostro computer durante una scansione.

Potete personalizzare la **Real-time protection** cliccando **Custom level**. Apparirà la seguente finestra:

Impostazioni Virus Shield

Le opzioni di scansione sono organizzate come menu espandibili, molto simili a quelli di esplorazione di Windows. Selezionare la casella con "+" per aprire un'opzione oppure la casella con "-" per chiudere un'opzione.

Nota

Si può vedere come alcune opzioni di scansione, nonostante appaia il segno "+", non possano essere aperte. Il motivo è che queste opzioni non sono ancora state selezionate. Si può notare che sarà possibile aprirle una volta selezionate.

- **Scansione dei file acceduti e dei trasferimenti P2P** - esamina i file acceduti e le comunicazioni tramite applicazioni Software di Messaggistica Istantanea (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Successivamente selezionare il tipo di file che si desidera esaminare.

Opzione		Descrizione
Esamina i files acceduti	**Tutti i file**	Verranno esaminati tutti i file acceduti, indipendentemente dalla loro tipologia.
	Scansiona solo applicazioni	Verranno esaminati solo i file di programma. Questo significa solo i file con le seguenti estensioni: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`;

Opzione		Descrizione
		.doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml e .nws.
	Estensioni definite dall'utente	Verranno esaminati soltanto i file con le estensioni specificate dall'utente. Le varie estensioni devono essere separate da ";".
	Scansione per riskware	Esamina alla ricerca di riskware. Questi file verranno trattati come file infetti. Software che includono componenti adware potrebbero bloccarsi se questa opzione è attiva. Seleziona **Ignora dialer e applicazioni durante la scansione** e/o **Ignora keylogger durante la scansione** se si desidera escludere questi tipi di file dalla scansione.
Scansiona solo i file nuovi e modificati		Scansiona solo i file che non sono stati scansionati in precedenza o che sono stati cambiati dall'ultima scansione. Selezionando questa opzione, è possibile migliorare di molto la risposta generale del sistema con un minimo compromesso per la sicurezza.
Esamina settore di boot		Per esaminare i settori di avvio del sistema.
Esamina gli archivi		Verranno esaminati anche gli archivi acceduti. Con questa opzione abilitata, il computer sarà più lento. È possibile impostare la dimensione massima di archivi da scansionare (in kilobyte, digitare 0 se si vogliono scansionare tutti gli archivi) e la profondità massima di archivi da scansionare.
Prima azione		Seleziona dal menù delle opzioni la prima azione da intraprendere su files infetti o sospetti:
	Rifiuta l'accesso e continua	Nel caso di individuazione di un file infetto, l'accesso al file verrà negato.

Opzione		Descrizione
	Disinfetta i file	Rimuove il codice malware da file infetti.
	Cancella file	Cancella immediatamente i file infetti, senza alcun avviso.
	Muovi file nella Quarantena	Sposta i file infetti nella zona di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.
Seconda azione		Seleziona la seconda azione dalle opzioni da intraprendere sui files infetti, nel caso in cui la prima fallisse.
	Rifiuta l'accesso e continua	Nel caso di individuazione di un file infetto, l'accesso al file verrà negato.
	Cancella file	Cancella immediatamente i file infetti, senza alcun avviso.
	Muovi file nella Quarantena	Sposta i file infetti nella zona di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.
Non scansionare i file più grandi di [x] Kb		Digitare la dimensione massima dei files da esaminare. Se la dimensione è pari a 0 Kb, tutti i files verranno esaminati.
Scansionare condivisioni di rete	**Tutti i file**	Verranno scansionati tutti i file acceduti dalla rete, indipendentemente dalla loro tipologia.
	Scansiona solo applicazioni	Verranno esaminati solo i file di programma. Questo significa solo i file con le seguenti estensioni: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml` e `.nws`.
	Estensioni definite dall'utente	Verranno esaminati soltanto i file con le estensioni specificate dall'utente. Le varie estensioni devono essere separate da ";".

- **Esamina il traffico e-mail** - tutti i messaggi e-mail vengono esaminati.

  Sono disponibili le seguenti opzioni:

Opzione	Descrizione
Esamina le e-mail in ingresso	Tutte le e-mail in ingresso vengono esaminate.
Esamina le e-mail in uscita	Tutte le e-mail in uscita vengono esaminate.

- **Scansiona il traffico web (HTTP)** - tutto il traffico http viene scansionato.
- **Mostra avviso, se viene rilevato un virus** - verrà visualizzata una finestra di avviso quando verrà rilevato un virus in un file o in un messaggio e-mail.

  In caso di file infetto, la finestra di avviso mostrerà il nome del virus, la situazione e l'azione intrapresa nei confronti del file infetto. In caso di email infetta, la finestra di avviso conterrà anche le informazioni riguardanti il mittente e il ricevente.

  In caso che un file sospetto è scansionati, puoi lanciare un wizard dalla finestra di allerta che ti aiuterà a spedire il file ai Laboratori Acronis per una ulteriore analisi. È possibile scrivere dalla tua e-mail per ricevere informazioni su questo report.
- **Esamina file ricevuti/inviati tramite IM.** Per esaminare i file che ricevete o inviate usando Yahoo Messenger o Windows Live Messenger, selezionare la casella corrispondente.

Selezionare **OK** per salvare le modifiche e chiudere la finestra.

17.1.3. Configurazione Active Virus Control

Acronis Backup and Security 2010 Active Virus Control fornisce un livello di protezione contro nuove minacce le cui firme non sono ancora state rilasciate. Analizza e monitora costantemente il comportamento delle applicazione in esecuzione sul vostro computer e vi avverte se una di queste ha un comportamento sospetto.

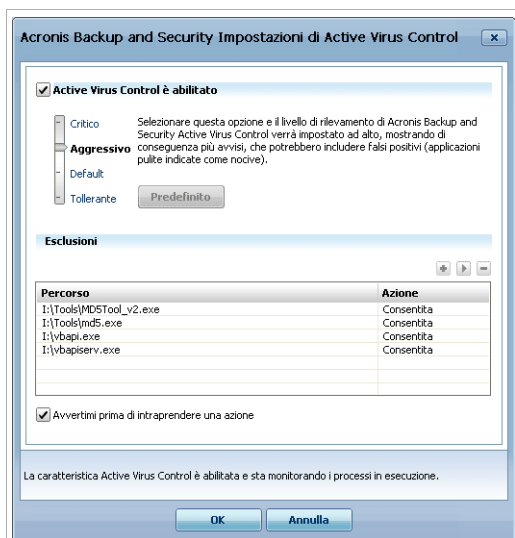
AVC può essere configurato per avvisare e richiedere un'azione dell'utente ogni volta che un'applicazione prova a compiere un'azione potenzialmente nociva.

Avviso Active Virus Control

Se conoscete e vi fidate dell'applicazione rilevata, cliccare su **Consentire**.

Se volete chiudere immediatamente l'applicazione, cliccare su **OK**.

Selezionare la casella di controllo **Ricorda questa azione per questa applicazione** prima di eseguire la propria scelta e Acronis Backup and Security 2010 eseguirà la stessa azione per l'applicazione rilevata in futuro. La regola creata viene elencata nella finestra di configurazione Active Virus Control,

Per configurare Active Virus Control, fare clic su **Impostazioni Avanzate**.

Impostazioni Active Virus Control

Selezionare la casella di controllo corrispondente per abilitare Active Virus Control.

Importante

Mantenere Active Virus Control abilitato per essere protetti contro virus sconosciuti.

Se si desidera ricevere avvisi e richieste di azione da parte di Active Virus Control quando una applicazione tenta di eseguire una possibile azione nociva, selezionare la casella di controllo **Chiedi cosa fare**.

Configurazione del Livello di Protezione

Il livello di protezione di AVC cambia automaticamente quando viene impostato un nuovo livello di protezione in tempo reale. Se non siete soddisfatti delle impostazioni di default, potete configurare manualmente il livello di protezione.

Nota

Tenere presente che se viene cambiato il livello corrente di protezione in tempo reale, il livello di protezione di AVC cambierà di conseguenza. Se si imposta la protezione in tempo reale su **Permissiva**, Active Virus Control viene disabilitato automaticamente. In questo caso è possibile abilitarlo manualmente quando si desidera usarlo.

Trascinate il pulsante scorrevole lungo la barra per impostare il livello di protezione che meglio si adatta alle vostre esigenze di sicurezza.

Livello di protezione	Descrizione
Critico	Controllo rigido di tutte le applicazioni alla ricerca di possibili azioni nocive.
Default	Il tasso di rilevamento è elevato e sono possibili dei falsi positivi.
Medio	Controllo dell'applicazione moderato, sono ancora possibili dei falsi positivi.
Permissiva	I tassi di rilevamento sono bassi e non vi sono falsi positivi.

Gestione delle Applicazioni Affidabili / Non affidabili

È possibile aggiungere applicazioni note e affidabili all'elenco di applicazioni affidabili. Queste applicazioni non verranno più controllate da Active Virus Control e verrà concesso loro accesso automaticamente.

Le applicazioni per cui sono state create delle regole vengono elencate nella tabella alla voce **Esclusioni**. Per ciascuna regola viene visualizzato il percorso dell'applicazione e l'azione impostata (Permessa o Bloccata).

Per modificare l'azione per un'applicazione fare clic sull'azione attuale e selezionare la nuova azione dal menu.

Per gestire l'elenco utilizzare i pulsanti posizionati al di sotto della tabella:

- **Aggiungi** - per aggiungere una nuova applicazione alla lista.

- **Rimuovi** - per rimuovere una applicazione dalla lista.
- **Modifica** - modifica una regola di applicazione.

17.1.4. Disattivazione Protezione in Tempo Reale

Se volete disattivare la protezione in tempo reale, apparirà la seguente finestra di avviso: Dovrete confermare la vostra scelta selezionando dal menu, per quanto tempo volete disattivare la protezione in tempo reale. Potete disattivarla durante 5, 15 o 30 minuti, un'ora, permanentemente o fino al riavvio del sistema.

Avvertimento

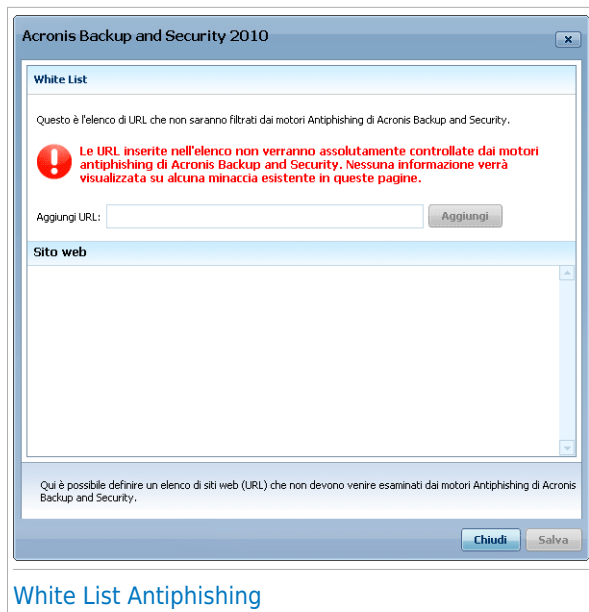
Questa è una questione di sicurezza critica. Vi consigliamo di disattivare la protezione in tempo reale per il minimo tempo possibile. Se la protezione in tempo reale non è attiva, non sarete protetti dalle minacce malware.

17.1.5. Configurazione della Protezione Antiphishing

Acronis Backup and Security 2010 fornisce protezione antiphishing in tempo reale per:

- Internet Explorer
- Mozilla Firefox
- Yahoo! Messenger
- Windows Live (MSN) Messenger

Potete scegliere di disabilitare la protezione antiphishing completamente o solo per applicazioni specifiche.

Potete cliccare su **White List** per configurare e gestire un elenco di pagine web che non devono essere esaminate dai motori Antiphishing Acronis Backup and Security 2010.

White List Antiphishing

Potete vedere i siti web che Acronis Backup and Security 2010 non controlla attualmente per contenuti phishing.

Per aggiungere un sito alla White List, inserire il suo indirizzo url nel campo corrispondente **Nuovo indirizzo** quindi cliccare **Aggiungi**. La white list dovrebbe contenere solo siti web di cui vi fidate completamente. Ad esempio, aggiungere siti web dove fate di solito i vostri acquisti online.

Nota

Potete aggiungere facilmente dei siti web alla White List utilizzando la barra degli strumenti Antiphishing Acronis integrata nel vostro browser. Per ulteriori informazioni, fare riferimento a *«Integrazione nei Web Browser»* (p. 275).

Per rimuovere un sito web dalla white list, fare clic sul pulsante corrispondente **Rimuovi**.

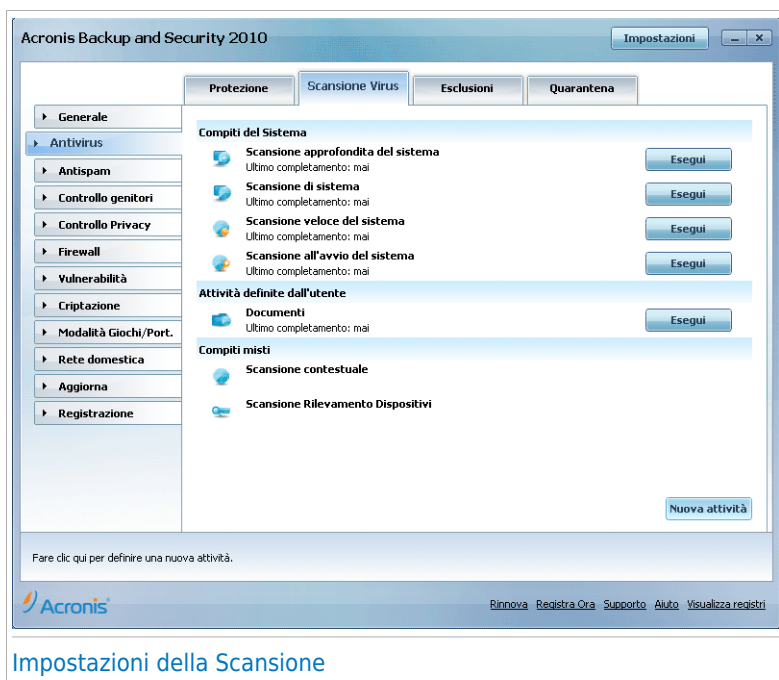
Fare clic su **Salva** per salvare le modifiche e chiudere la finestra.

17.2. Scansione a richiesta

L'obiettivo principale di Acronis Backup and Security 2010 è di mantenere il vostro computer privo di virus. Ciò avviene principalmente tenendo lontani i nuovi virus

dal vostro computer ed esaminando i vostri messaggi e-mail e qualsiasi nuovo file scaricato o copiato sul vostro sistema.

Esiste il rischio che un virus sia già contenuto nel vostro sistema, addirittura prima dell'installazione di Acronis Backup and Security 2010. Questo è il motivo per cui suggeriamo di effettuare una scansione sul vostro computer alla ricerca di virus residenti dopo aver installato Acronis Backup and Security 2010. Inoltre di effettuare frequentemente una scansione del vostro computer alla ricerca di virus.

Per configurare ed avviare la scansione a richiesta, fare clic su **Antivirus>Virus Scan** nella Modalità Avanzata.

Impostazioni della Scansione

La scansione a richiesta si basa sulle impostazioni della scansione. Le impostazioni della scansione specificano le opzioni della scasione e gli oggetti da esaminare. Potete esaminare il vostro computer in qualsiasi momento, eseguendo le funzioni predefinite oppure le vostre (definite dall'utente). Potete anche programmarle affinchè vengano eseguite con cadenza regolare oppure quando il sistema è inattivo in modo da non interferire con il vostro lavoro.

17.2.1. Impostazioni della Scansione

Acronis Backup and Security 2010 ha tante funzioni, create per default, che coprono i problemi di sicurezza comuni. Voi potete anche creare le vostre funzioni di scansione personalizzate.

Vi sono tre categorie di compiti di scansione:

- **Funzioni di Sistema** - contiene la lista delle funzioni di sistema di default. Sono disponibili i compiti seguenti:

Funzione di Default	Descrizione
Scansione del Sistema approfondita	Esamina l'intero sistema. Nella configurazione predefinita, esegue la scansione per tutti i tipi di malware che minacciano la sicurezza del vostro sistema, come virus, spyware, adware, rootkits ed altri.
Scansione sistema	Esamina l'intero sistema, esclusi gli archivi. Nella configurazione di default la scansione ricerca tutti i tipi di malware ad eccezione dei rootkit.
Scansione Veloce del Sistema	Scansiona le cartelle `Windows` e `Program Files`. Nella configurazione predefinita, esamina per cercare tutti i tipi di malware, esclusi i rootkit, ma non esamina la memoria, il registro nè i cookies.
Scansione accesso automatico	Esamina gli elementi che vengono eseguiti quando un utente accede a Windows. Di default, la scansione autologon è disabilitata Se si vuole utilizzare questa attività, fare clic con il pulsante destro e selezionare **Programma** e impostare l'attività per l'esecuzione **all'avvio del sistema**. Specifica dopo quanto tempo dal suo inizio, il compito deve essere fermato.

Nota

Poiché le funzioni **Scansione approfondita del sistema** e **Scansione completa del sistema** analizzano l'intero sistema, la scansione può richiedere un po' di tempo. Quindi consigliamo di eseguire questi compiti con priorità bassa o, meglio, quando il sistema è inattivo.

- **Impostazione Utente** - contiene le impostazioni definite dall'utente.

  Viene fornita una funzione chiamata `My Documents`. Utilizzare questa funzione per esaminare delle cartelle importanti dell'utente corrente: `My Documents`,

`Desktop` e `StartUp`. Questo garantirà la sicurezza dei vostri documenti, uno spazio di lavoro sicuro ed applicazioni pulite al avvio.

- **Compiti misti** - contiene un elenco di compiti di scansione misti. Questi compiti di scansione si riferiscono a tipi di scansione alternativi che non possono essere eseguiti da questa finestra. Potete solo modificare le loro impostazioni o vedere i report delle scansioni.

Ogni attività ha una finestra **Proprietà** che ne permette la configurazione e la visualizzazione dei registri di scansione. Per aprire tale finestra fare doppio clic sul pulsante **Proprietà** prima del nome dell'attività. Per ulteriori informazioni fare riferimento a *«Configurare un Compito di Scansione»* (p. 130).

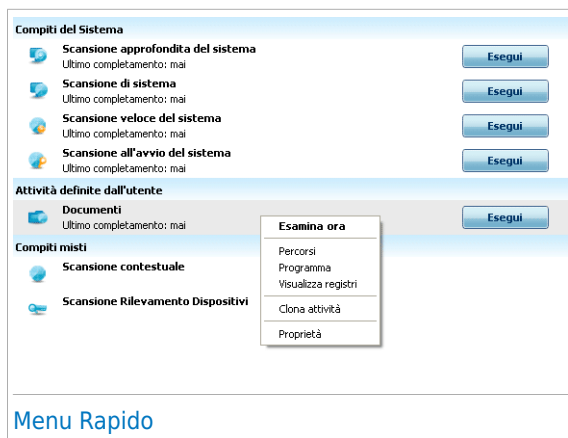
Per eseguire una scansione di sistema o definita dall'utente, fare clic sul pulsante **Esegui Attività** corrispondente. La Procedura guidata scansione antivirus apparirà e guiderà attraverso il processo di scansione.

Quando un'attività è programmata per essere eseguita automaticamente, in un momento successivo o regolarmente, viene visualizzato il pulsante **Programma** a destra dell'attività. Fare clic su questo pulsante per aprire la finestra **Proprietà**, scheda Programmazione, dove è possibile vedere e modificare il programma dell'attività.

Se non è più necessaria un'attività di scansione creata (definita dall'utente), è possibile cancellare facendo clic sul pulsante **Elimina**, a destra dell'attività. Non è possibile rimuovere attività varie o di sistema.

17.2.2. Utilizzo del Menu Rapido

Un menu rapido è disponibile per ciascun compito. Cliccare col pulsante destro del mouse sul compito selezionato per aprirlo.

Menu Rapido

Per le attività di sistema e definite dall'utente sono disponibili i seguenti comandi nel menu di scelta rapida:

- **Scan Now** - esegue la funzione selezionata, avviando immediatamente una scansione.
- **Target di Scansione** - apre la sezione Percorso Scansione nella finestra delle **Proprietà**, dove potete cambiare il target di scansione per i compiti selezionati.

Nota

Nel caso di funzioni del sistema, questa opzione viene sostituita da **Mostrare percorsi delle scansioni**, dato che è possibile vedere solo il loro target di scansione.

- **Schedule** - apre la**Finestra proprietà** Programma tab, dove puoi programmare i compiti selezionati.
- **Visualizza registri** - apre la finestra **Proprietà**, scheda Registri dove è possibile vedere i report generati dopo che l'attività selezionata è stata eseguita.
- **Attività di clonazione** - duplica l'attività selezionata. Ciò è utile quando si creano nuovi compiti, in quanto potete modificare le impostazioni del compito duplicato.
- **Cancella** - cancella i compiti selezionati.

Nota

Non disponibile per compiti di sistema. Non potete rimuovere un compito di sistema.

- **Proprietà** - apre la finestra **Proprietà**, scheda Panoramica, dove è possibile cambiare le impostazioni dell'attività selezionata.

Data la particolare natura della categoria **Attività varie** solo le opzioni **Visualizza registri** e **Proprietà** sono disponibili in questo caso.

17.2.3. Creazione delle Funzioni di Scansione

Per creare un compito di scansione, utilizzare uno di questi metodi:

- Duplica una attività esistente, rinominala ed apporta le modifiche necessarie nella finestra delle Proprietà.
- Cliccare **Nuovo Compito** per creare un nuovo compito e configurarlo.

17.2.4. Configurare un Compito di Scansione

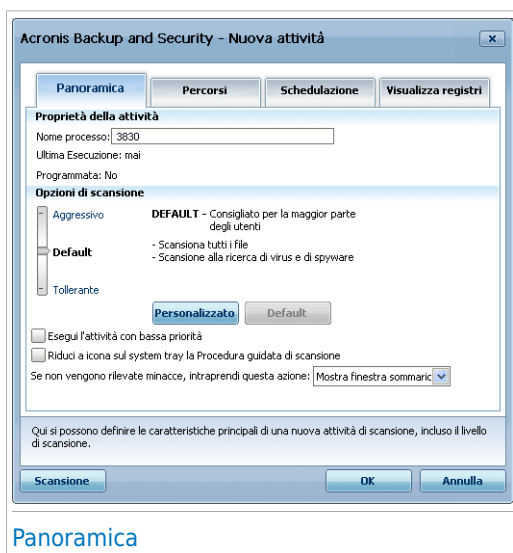
Ogni compito di scansione ha la sua propria finestra delle **Proprietà**, dove potete configurare le opzioni di scansione, impostare il target della scansione, programmare il compito o vedere i report. Per aprire questa finestra fare clic sul pulsante **Proprietà**

alla sinistra dell'attività (o fare clic con il pulsante destro sull'attività e poi fare clic su **Proprietà**). E' anche possibile fare doppio clic sull'attività.

Nota
Per ulteriori informazioni sulla visualizzazione dei registri e sulla funzione **Visualizza Registri**, fare riferimento a *«Visualizzazione dei Registri di Scansione»* (p. 150).

Configurazione delle Impostazioni di Scansione

Per configurare le opzioni di scansione di un'attività specifica, fare clic con il pulsante destro e selezionare**Proprietà**. Apparirà la finestra seguente:

Panoramica

Qui potete vedere le informazioni sul compito (nome, ultima esecuzione e stato della programmazione) ed impostare le impostazioni di scansione.

Scelta del Livello di Scansione

Potete facilmente configurare le impostazioni di scansione scegliendo il livello di scansione. Trascinare l'indicatore sulla barra per impostare l'appropriato livello di scansione.

Ci sono 3 livelli di scansione:

Livello di protezione	Descrizione
Permissiva	Offre un'efficienza di rilevamento ragionevole. Il livello di consumo delle risorse è basso.

Livello di protezione	Descrizione
	Vengono esaminati alla ricerca di virus solo i programmi. Oltre alla classica scansione basata sulla firma, è utilizzata anche l'analisi euristica.
Medio	Offre una buona efficienza di rilevamento. Il livello di consumo delle risorse è moderato. Tutti i file vengono esaminati alla ricerca di virus e spyware. Oltre alla classica scansione basata sulle impronte, è utilizata anche l'analisi euristica.
Aggressiva	Offre un'alta efficienza di rilevamento. Il livello di consumo di risorse è alto. Tutti i file e gli archivi vengono esaminati alla ricerca di virus e spyware. Oltre alla classica scansione basata sulle impronte, è utilizzata anche l'analisi euristica.

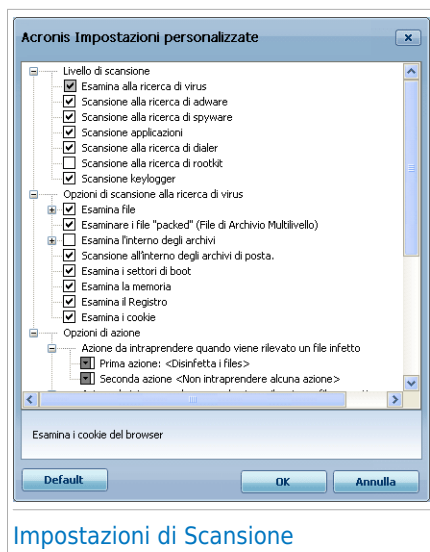
È anche disponibile una serie di opzioni generali per il processo di scansione:

- **Esegui il task di scansione con Bassa Priorità.** Riduce la priorità del processo di scansione. Permetterai ad altri programmi di essere più veloci ed incrementerai il tempo necessario per finire il processo di scansione.
- **Minimizza la finestra di scansione nel systray.** Riduce a icona la finestra di scansione sulla barra degli strumenti. Eseguire un doppio clic sull'icona di Acronis per riaprirla.
- **Spegnere il computer quando la scansione sia completata e non siano state rilevate delle minacce**

Selezionare **OK** per salvare le modifiche e chiudere la finestra. Per eseguire la funzione, selezionare **Scansione**.

Personalizzazione del Livello di Scansione

Gli utenti esperti possono trarre vantaggio dalle possibilità di impostazione della scansione Acronis Backup and Security 2010. Infatti la scansione può essere impostata in modo di esaminare solo delle specifiche estensioni, di cercare delle particolare minacce malware, o di non esaminare gli archivi. Questo può ridurre di molto i tempi di scansione ed incrementare la reattività del vostro computer durante una scansione.

Cliccare su **Personalizza** per impostare le vostre opzioni di scansione. Si aprirà una nuova finestra.

Impostazioni di Scansione

Le opzioni di scansione sono organizzate come menu espandibili, molto simili a quelli di esplorazione di Windows. Selezionare la casella con "+" per aprire un’opzione oppure la casella con "-" per chiudere un’opzione.

Le opzioni di scansione sono raggruppate in 3 categorie:

- **Livello di Scansione.** Specificare il tipo di malware che volete che Acronis Backup and Security 2010 analizzi, selezionando le opzioni appropriate dalla categoria **Livello di scansione**.

Opzione	Descrizione
Scansione Virus	Esamina per virus conosciuti. Acronis Backup and Security 2010 rileva anche virus incompleti, rimuovendo ogni possibile minaccia che possa colpire la sicurezza del vostro sistema.
Scansione adware	Esegue la scansione per minacce adware. Questi file verranno trattati come file infetti. Software che includono componenti adware potrebbero bloccarsi se questa opzione è attiva.
Scansione spyware	Esegue la scansione per minacce spyware conosciuti. Questi file verranno trattati come file infetti.

Opzione	Descrizione
Scansione applicazione	Cerca applicazioni legittime che possono essere usate come strumenti per spiare, per nascondere applicazioni maligne o per altri intenti maligni.
Scansione dialers	Esegue la scansione per applicazioni che utilizzano numeri di telefono a costo elevato. Questi file verranno trattati come file infetti. Software che includono componenti dialer potrebbero bloccarsi se questa opzione fosse attiva.
Scansione per i Rootkits	Esegue la scansione per oggetti nascosti (file e processi), generalmente conosciuti come rootkits.

- **Opzioni di scansione virus.** Specificare il tipo di oggetti da esaminare (tipi di file, archivi e così via) selezionando opzioni appropriate dalla categoria **Opzioni di scansione virus**.

Opzione		Descrizione
Esamina file	**Tutti i file**	Verranno esaminati tutti i file, indipendentemente dalla loro tipologia.
	Esaminare solo i program file	Per esaminare soltanto i file di programma. Ciò significa solo i file con le seguenti estensioni: exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; exe; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml e nws.
	Estensioni definite dall'utente	Verranno esaminati soltanto i file con le estensioni specificate dall'utente. Le varie estensioni devono essere separate da ";".
Esamina i programmi impaccati		Per esaminare i file impaccati.
Esamina gli archivi		Scansiona negli archivi regolari, tipo .zip, .rar, .ace, .iso e altri. Selezionare la casella di controllo **Scansiona programmi di installazione e archivi chm** se si desidera scansionare questo tipo di file. La scansione dei file archiviati incrementa il tempo di scansione e richiede più risorse di

Opzione	Descrizione
	sistema. È possibile impostare una dimensione massima di archivi da scansionare in kilobyte (KB) digitando la dimensione in questo campo **Limite di dimensione degli archivi da scansionare**.
Scansionare gli archivi di e-mail	Per eseguire la scansione all'interno degli archivi di posta.
Esamina settore di boot	Per esaminare i settori di avvio del sistema.
Scansione della memoria	Scansiona la memoria alla ricerca di virus e altro malware.
Scansione registro	Scansione di voci di registro.
Scansionare cookies	Scansione di file cookie.

- **Opzioni di azione.** Specificare le azioni da intraprendere per ogni categoria dei file rilevati usando le opzioni in questa categoria.

Nota

Per impostare una nuova azione, fare clic sulla **Prima azione** attuale e selezionare l'opzione desiderata dal menu. Specificare una **Seconda azione** che sarà intrapresa qualora la prima non riuscisse.

▶ Selezionare l'azione da intraprendere sui file infetti rilevati. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file infetti. Questi file appariranno nel file di rapporto.
Disinfetta i file	Rimuovere il codice malware dai file infetti rilevati.
Cancella i file	Cancella immediatamente i file infetti, senza alcun avviso.
Muova i files in Quarantena	Sposta i file infetti nella zona di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.

▶ Selezionare l'azione da intraprendere sui file sospetti rilevati. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file sospetti. Questi file appariranno nel file di report.
Cancella i file	Cancella immediatamente i file sospetti, senza alcun avviso.
Muova i files in Quarantena	Sposta i file sospetti nella zona di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.

Nota

La Scansione euristica ha rilevato dei file sospetti. Vi consigliamo di inviarli al laboratorio di Acronis.

▶ Selezionare l'azione da intraprendere sugli oggetti nascosti (rootkits) rilevati. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file nascosti. Questi file appariranno nel file di report.
Rinomina i files	Cambia il nome di file nascosti aggiungendo `.bd.ren` al loro nome. Come risultato, si potrà cercare tali file sul computer, se ve ne sono.
Muova i files in Quarantena	Sposta i file nascosti nella zona di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.

Nota

Notare che i file nascosti non sono i file che l'utente ha nascosto in modo deliberato da Windows. Sono file nascosti da programmi speciali, noti come rootkit. I rootkit non sono file di tipo nocivo. Tuttavia sono utilizzati per rendere introvabili virus o spyware per normali programmi antivirus.

▶ **Opzioni per file protetti da password e criptati.** File criptati utilizzando Windows potrebbero essere importanti. Ecco perché è possibile configurare differenti azioni da intraprendere per file infetti o sospetti che sono criptati utilizzarti Windows. Un'altra categoria di file che richiede azioni speciali sono gli archivi protetti da password. Gli archivi protetti da password non possono essere esaminati a meno che non forniate la password. Utilizzare queste opzioni per configurare le azioni da intraprendere per archivi protetti da password e per file criptati con Windows.

– **Azione da intraprendere quando viene rilevato un file criptato infetto.** Selezionare l'azione da intraprendere su file infetti criptati usando Windows. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Non eseguire alcuna Azione	Registra solamente i file infetti che sono criptati utilizzando Windows. Dopo che la scansione sia stata completata, potrete aprire il log di scansione per visualizzare le informazioni su questi file.
Disinfetta i file	Rimuovere il codice malware dai file infetti rilevati. La disinfezione può fallire in alcuni casi, come quando il file infetto è all'interno di specifici archivi di posta.
Cancella i file	Rimuovere immediatamente dal disco i file infetti, senza alcun avviso.
Muova i files in Quarantena	Spostare i file infetti dalla loro posizione originale alla cartella di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.

– **Azione da intraprendere quando viene rilevato un file criptato sospetto.** Selezionare l'azione da intraprendere su file sospetti criptati usando Windows. Sono disponibili le seguenti opzioni:

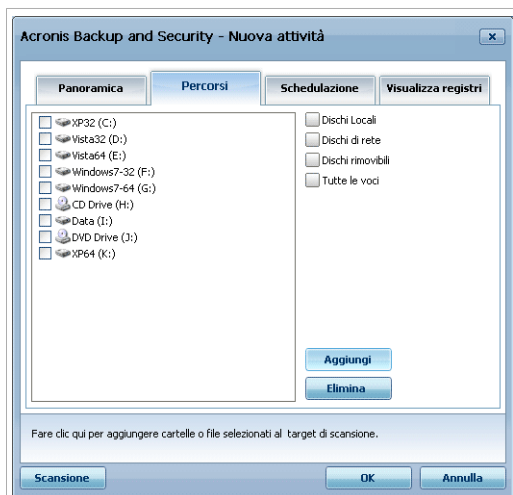
Azione	Descrizione
Non eseguire alcuna Azione	Registra solamente i file sospetti che sono criptati utilizzando Windows. Dopo che la scansione sia stata completata, potrete aprire il log di scansione per visualizzare le informazioni su questi file.
Cancella i file	Cancella immediatamente i file sospetti, senza alcun avviso.
Muova i files in Quarantena	Sposta i file sospetti nella zona di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.

– **Azione da intraprendere quando viene rilevato un file protetto da password.** Selezionare l'azione da intraprendere sui file protetti da password rilevati. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Registra solo	Tenere registro solo dei file protetti da password nel log di scansione Dopo che la scansione sia stata completata, potrete aprire il log di scansione per visualizzare le informazioni su questi file.
Chiedere password	Quando viene rilevato un file protetto da password, chiedere all'utente di fornire la password per poter esaminare il file.

Se clicchi su **Predefinito** verranno applicate le impostazioni di default. Selezionare **OK** per salvare le modifiche e chiudere la finestra.

Impostazione del Target di Scansione

Per impostare il target di scansione a una attività di scansione specifica di un utente, fare clic con il pulsante di destra e selezionare **Percorsi**. Alternativamente, se si è già nella finestra Proprietà di un'attività, selezionare la scheda **Percorsi**. Apparirà la finestra seguente:

Target di scansione

Potete vedere la lista di dischi locali, di rete e rimuovibili, ed anche i file e cartelle aggiunti in precedenza, se ci sono. Tutti gli oggetti selezionati verranno esaminati all'esecuzione della funzione.

Sono disponibili i seguenti tasti:

- **Aggiungi Oggetti** - apre una finestra di visualizzazione dove è possibile selezionare i file o le cartelle che si desidera esaminare.

Nota

Utilizzare seleziona & trascina per aggiungere file/cartelle all'elenco.

- **Cancellare Oggetti** - rimuove il (i) file / cartella(e) precedentemente selezionati dall'elenco degli oggetti da esaminare.

Nota

Possono essere cancellati solo i file / cartelle aggiunti successivamente e non quelli "visti" automaticamente da Acronis Backup and Security 2010.

Oltre a questi pulsanti, vi sono altre opzioni che permettono la selezione veloce delle posizioni di scansione.

- **Dischi locali** - per esaminare i drives locali.
- **Dischi di rete** - per esaminare tutti i drive di rete.
- **Drive Rimovibili** - per esaminare i drive rimovibili (CD-ROM, floppy-disk).
- **Tutti gli elementi** - per esaminare tutti i drive, indipendentemente dal fatto che siano locali, sulla rete o rimovibili.

Nota

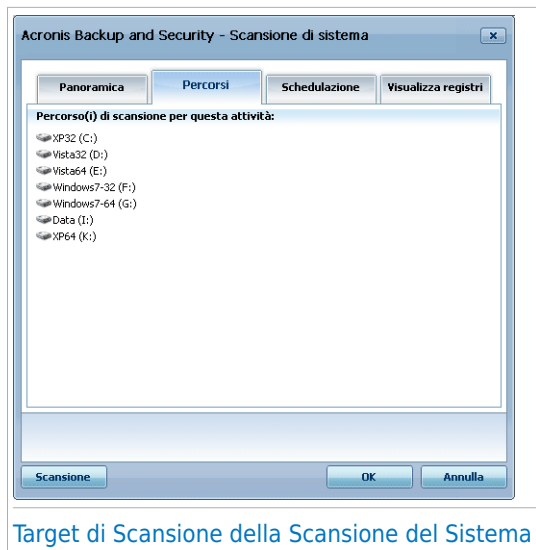
Se desiderate eseguire una scansione di tutto il vostro computer alla ricerca di virus, selezionare la casella corrispondente a **Tutti gli elementi**.

Selezionare **OK** per salvare le modifiche e chiudere la finestra. Per eseguire la funzione, selezionare **Scansione**.

Visualizzazione del Target di Scansione delle Funzioni del Sistema

Non è possibile modificare il target di scansione delle attività di scansione dalla categoria **Attività di Sistema**. Potete solo visualizzare il loro target di scansione.

Per visualizzare il target di scansione di una specifica attività di scansione del sistema, fare clic con il tasto destro sull'attività e selezionare **Mostra Percorsi di Scansione**. Per **Scansione del sistema**, ad esempio, apparirà la seguente finestra:

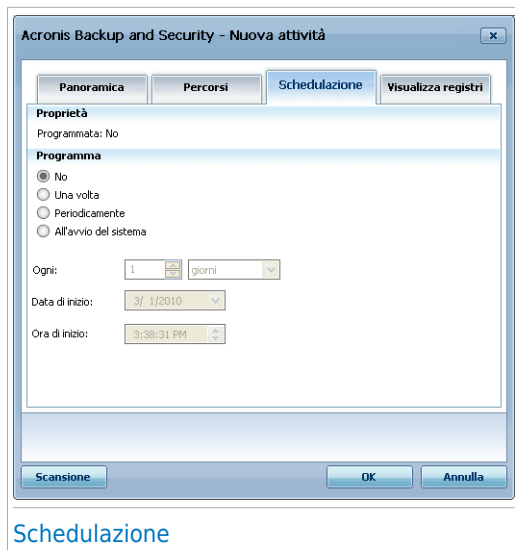
Target di Scansione della Scansione del Sistema

Scansione del sistema e **Scansione approfondita del sistema** scansioneranno tutti i drive locali, mentre **Scansione veloce del sistema** scansionerà solo le cartelle `Windows` e `Program Files`.

Selezionare **OK** per chiudere la finestra. Per eseguire la funzione, cliccare semplicemente **eseguire scansione**.

Programmazione delle Funzioni di Scansione

Una scansione completa può richiedere un certo tempo e agisce meglio se vengono chiusi tutti gli altri programmi. La miglior cosa da fare è programmare la scansione nel momento in cui il vostro computer non viene utilizzato.

Per vedere il programma di un'attività specifica o per modificarlo, fare clic con il pulsante destro sull'attività e selezionare **Programmazione**. Se si è già nella finestra Proprietà dell'attività, selezionare la scheda **Utilità di pianificazione**. Apparirà la finestra seguente:

Schedulazione

Potete vedere la programmazione delle funzioni, se ci sono.

Quando programmate un compito, dovete scegliere una delle seguenti opzioni:

- **No** - lancia la scansione solo quando richiesta dall'utente.
- **Una volta** - lancia la scansione solo una volta, in un certo momento. Specificare la data e l'ora di avvio nel campo **Start Date/Time**.
- **Periodicamente** - lancia la scansione periodicamente, a certi intervalli di tempo (minuti, ore, giorni, settimane, mesi) iniziando da una certa data ed ora specificate.

  Se si desidera che la scansione venga ripetuta a determinati intervalli, selezionare la casella corrispondente a **Periodicamente** e digitare nel campo **Ogni** il numero di minuti / ore / giorni / settimane / mesi indicando la frequenza del processo. È inoltre necessario specificare la data e l'ora di inizio nei campi **Data/Ora di inizio**.
- **All'avvio del sistema** - lancia la scansione un numero specifico di minuti dopo che l'utente ha effettuato l'accesso a Windows.

Selezionare **OK** per salvare le modifiche e chiudere la finestra. Per eseguire la funzione, selezionare **Scansione**.

17.2.5. Scansione file e cartelle

Prima di iniziare il processo di scansione, assicurarsi che Acronis Backup and Security 2010 sia aggiornato con le firme malware. Eseguire la scansione usando un database delle impronte obsoleto può impedire Acronis Backup and Security 2010 di rilevare

nuovo malware, trovato dopo l'ultimo aggiornamento. Per verificare quando è stato eseguito l'ultimo aggiornamento, fare clic su **Aggiornamento>Aggiornamento** in Modalità avanzata.

Nota

Per consentire a Acronis Backup and Security 2010 di eseguire una scansione completa, dovrete chiudere tutti i programmi aperti. E' soprattutto importante chiudere il vostro client di posta (come Outlook, Outlook Express oppure Eudora).

Consiglio di scansione

Ecco altri consigli sulla scansione che potrebbero essere utili:

- In base alla dimensione del disco rigido, l'esecuzione di una scansione comprensiva del computer (ad esempio una Scansione approfondita del sistema o una Scansione del sistema) potrebbe richiedere molto tempo (fino ad un ora o più). Quindi, si dovrebbero eseguire tali scansioni quando non si usa il computer per un lungo periodo di tempo (ad esempio di notte).

  È possibile programmare la scansione affinché inizi quando è più conveniente. Assicurarsi di lasciare il computer accesso. Con Windows Vista, assicurarsi che il computer non sia nella modalità sospensione quando l'attività deve essere eseguita.
- Se si scaricano spesso file da Internet ad una cartekka specifica, si consiglia di creare una nuova attività di scansione e impostare quella cartella come target della scansione. Programmare l'attività affinché venga eseguita una volta al giorno o più spesso.
- Esiste un malware che si imposta per essere eseguito ad ogni avvio del sistema modificando le impostazioni di Windows. Per proteggere il computer da un tale malware, è possibile programmare che l'attività **Scansioen accesso automatico** venga eseguito all'avvio del sistema. Notare che la scansione accesso automatico potrebbe influenzare la performance del sistema per un breve periodo di tempo dopo l'avvio.

Metodi di Scansione

Acronis Backup and Security 2010 consente quattro tipi di scansione a richiesta:

- Scansione immediata - avvia immediatamente un processo di scansione dal sistema / funzioni utente.
- Scansione contestuale - fare clic con il pulsante destro su un file o una cartella e selezionare **Scansione con Acronis Backup and Security**.
- Scansione Seleziona & Trascina - seleziona & trascina un file o una cartella sopra la Barra delle Attività di Scansione.
- Scansione manuale - Utilizzare Scansione Manuale di Acronis per selezionare direttamente i file o cartella da esaminare.

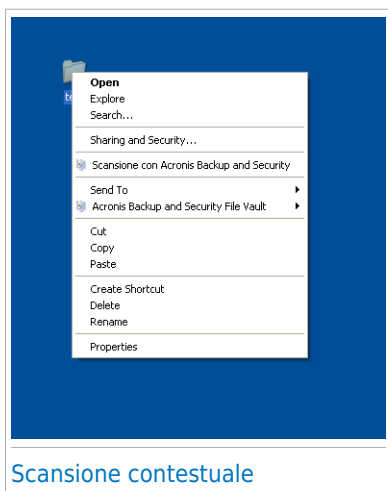
Scansione Immediata

Per eseguire una scansione del vostro computer o di parte di essi potete usare i compiti di scansione di default oppure i vostri propri compiti di scansione. Ciò si chiama scansione immediata

Per eseguire una scansione di sistema o definita dall'utente, fare clic sul pulsante **Esegui Attività** corrispondente. La Procedura guidata scansione antivirus apparirà e guiderà attraverso il processo di scansione.

Scansione Contestuale

Per esaminare un file o cartella senza configurare un nuovo compito di scansione, si può usare il menu contestuale. ciò si chiama scansione contestuale

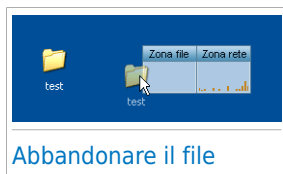
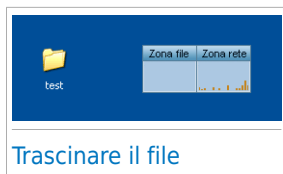
Scansione contestuale

Fare clic con il pulsante destro del mouse sul file o la cartella che si desidera scansionare e selezionare **Scansiona con Acronis Backup and Security**. La Procedura guidata scansione antivirus apparirà e guiderà attraverso il processo di scansione.

E' possibile modificare e vedere il file di report dalla finestra delle **Proprietà** del **Menu Scansione Contestuale**.

Scansione Seleziona e Trascina

Selezionare il file o la cartella che si desidera esaminare e trascinarla sulla **Barra delle Attività di Scansione**, come nella figura seguente.

Trascinare il file

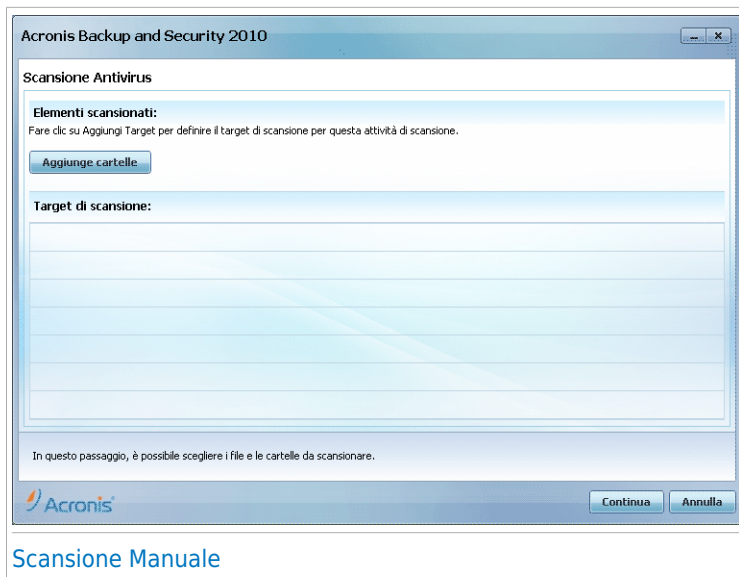
Abbandonare il file

La Procedura guidata scansione antivirus apparirà e guiderà attraverso il processo di scansione.

Scansione Manuale

La scansione manuale consiste in selezionare direttamente l'oggetto da esaminare, utilizzando l'opzione Scansione Manuale Acronis dal gruppo di programmi Acronis Backup and Security 2010 nel Menu di Avvio.

Nota

La scansione manuale è molto utile, poichè può essere eseguita anche quando Windows lavora in Modalità Provvisoria.

Per selezionare l'oggetto da scansionare con Acronis Backup and Security 2010, nel menu Avvio di Windows, seguire il percorso **Avvio** → **Programmi** → **Acronis** → **Acronis Backup and Security 2010** → **Scansione Manuale Acronis**. Apparirà la finestra seguente:

Scansione Manuale

Fare clic su **Aggiungi Cartella**, selezionare la posizione per cui si desidera eseguire la scansione e fare clic su **OK**. Se si desidera eseguire la scansione di cartelle multiple, ripetere questa azione per ciascuna posizione aggiuntiva.

I percorsi alle posizioni selezionate appariranno nella colonna **Target di Scansione**. Se si cambia idea circa la locazione, sarà sufficiente fare clic sul pulsante **Rimuovere** vicino. Fare clic sul pulsante **Rimuovi Tutti i Percorsi** per rimuovere tutte le posizioni aggiunte all'elenco.

Quando si ha concluso la selezione delle posizioni, fare clic su **Continua**. La Procedura guidata scansione antivirus apparirà e guiderà attraverso il processo di scansione.

Procedura guidata scansione antivirus

Quando si avvia la scansione su richiesta, apparirà la Procedura guidata Scansione Antivirus. Seguire la procedura di tre passi per completare il processo di scansione.

Nota

Se non appare la procedura guidata di scansione, potrebbe darsi che la procedura guidata sia configurata per una esecuzione sullo sfondo. Cercare l'icona di avanzamento della scansione nella barra delle applicazioni. Clicca su questa icona per aprire un processo di scansione e visualizzarne il progresso.

Passo 1/3 – Scansione

Acronis Backup and Security 2010 inizierà la scansione degli oggetti selezionati.

Scansione in corso

Potete visualizzare lo stato della scansione e le statistiche (velocità di scansione, tempo trascorso, numero di oggetti esaminati / infetti / sospetti / nascosti ed altro).

Attendere che Acronis Backup and Security 2010 finisca la scansione.

Nota

La durata del processo dipende dalla complessità della scansione.

Archivi protetti da password. Se Acronis Backup and Security 2010 rileva un archivio protetto da password durante la scansione e l'azione predefinita è **Richiedi la password**, verrà chiesto di inserire la password. Gli archivi protetti da password non possono essere esaminati a meno che non forniate la password. Sono disponibili le seguenti opzioni:

- **Password.** Se si desidera che Acronis Backup and Security 2010 scansioni l'archivio, selezionare questa opzione e digitare la password. Se non si conosce la password, scegliere un'altra opzione.
- **Non chiedere una password e ignorare questo oggetto durante la scansione.** Selezionare questa opzione per non scansionare questo archivio.

- **Ignora tutti gli elementi protetti da password senza scansionarli.** Selezionare questa opzione se non si vuole ricevere ulteriore domande sugli archivi protetti da password. Acronis Backup and Security 2010 non sarà in grado di scansionarli, ma verranno annotati nel registro della scansione.

Fare clic su **OK** per continuare la scansione.

Arresto o messa in pausa della scansione. Potete fermare la scansione in qualsiasi momento, cliccando su **Fermare**. Verrete portati all'ultimo passo dell'assistente. Per interrompere temporaneamente il processo di scansione, cliccare semplicemente su **Pausa**. Per riprendere la scansione dovrete cliccare su **Continuare**.

Passo 2/3 – Selezionare Azioni

Una volta completato il processo di scansione, apparirà una nuova finestra, dove potrete visualizzare i risultati della scansione.

Azioni

Si potrà vedere il numero di problemi che colpiscono il vs. sistema.

Gli oggetti infetti vengono mostrati in gruppi in base al malware con il quale sono stati infettati. Cliccare sul link corrispondente alla minaccia per trovare più informazioni sugli oggetti infetti.

Potete scegliere di intraprendere un'azione globale per tutti i problemi oppure selezionare azioni separate per ogni gruppo di problemi.

Una o più delle seguenti opzioni possono apparire nel menu:

Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file rilevati. Dopo che la scansione sia stata completata, potrete aprire il log di scansione per visualizzare le informazioni su questi file.
Disinfettare	Rimuove il codice malware da file infetti.
Eliminare	Elimina i file infetti.
Sposta in quarantena	Sposta i file infetti nella quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.
Rinomina i files	Cambia il nome di file nascosti aggiungendo `.bd.ren` al loro nome. Come risultato, si potrà cercare tali file sul computer, se ve ne sono. Notare che i file nascosti non sono i file che l'utente ha nascosto in modo deliberato da Windows. Sono file nascosti da programmi speciali, noti come rootkit. I rootkit non sono file di tipo nocivo. Tuttavia sono utilizzati per rendere introvabili virus o spyware per normali programmi antivirus.

Cliccare su **Continuare** per applicare le azioni specificate.

Passo 3/3 – Visualizzare risultati

Quando Acronis Backup and Security 2010 completa la risoluzione dei problemi, i risultati della scansione appariranno in una nuova finestra.

Riassunto

E' possibile visualizzare il sommario dei risultati. Se si desiderano informazioni esaurienti sul processo di scansione, fare clic su **Visualizza registro** per visualizzare il registro di scansione.

Importante

Se richiesto, vi preghiamo di riavviare il sistema per completare il processo di pulizia.

Cliccare su **Chiudere** per chiudere la finestra.

Acronis Backup and Security 2010 potrebbe non risolvere alcuni problemi

Nella maggior parte dei casi Acronis Backup and Security 2010 disinfetta con successo i file infetti che rileva o isola l'infezione. Comunque, ci sono dei problemi che non possono essere risolti.

In questi casi vi consigliamo di contattare il Team di supporto di Acronis su http://www.acronis.it/support/?ow=1. Il nostro team di supporto vi aiuterà a risolvere i vostri problemi.

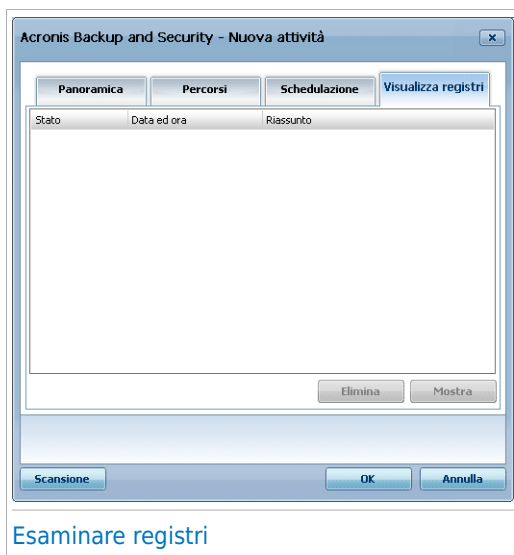
Acronis Backup and Security 2010 ha rilevato dei file sospetti

I file sospetti sono file rilevati dall'analisi euristica come potenzialmente infetti con malware la cui firma non è ancora stata rilasciata.

Se sono stati rilevati file sospetti durante la scansione, vi sarà richiesto di inviarli al Lab Acronis. Cliccare su **OK** per inviare questi file ai laboratori Acronis per ulteriori analisi.

17.2.6. Visualizzazione dei Registri di Scansione

Per visualizzare i risultati della scansione una volta completata un'attività, fare clic con il tasto destro sull'attività e selezionare **Visualizza Registri**. Apparirà la finestra seguente:

Esaminare registri

Qui potete trovare i file del report generati ogni che una funzione viene eseguita. In ogni file vengono fornite informazioni sullo stato del processo di scansione registrato, la data e l'ora in cui la scansione è stata eseguita ed un riassunto sui risultati della scansione.

Sono disponibili due pulsanti:

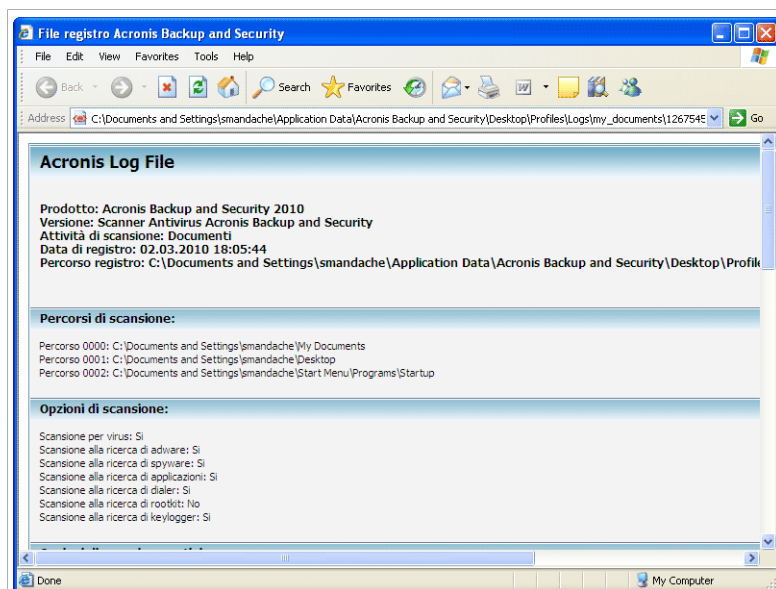
- **Cancellare** - per eliminare il log di scansione selezionato.
- **Mostrare** - per visualizzare il log di scansione selezionato. Il registro di scansione si aprirà nel vostro web browser predefinito.

Nota

Inoltre, per visualizzare o cancellare un file, fare clic con il pulsante destro sul file e selezionare l'opzione corrispondente dal menu di scelta rapida.

Selezionare **OK** per salvare le modifiche e chiudere la finestra. Per eseguire la funzione, selezionare **Scansione**.

Esempio di Registro di Scansione

La seguente figura rappresenta un esempio di registro di scansione:

Esempio di Registro di Scansione

Il log di scansione contiene informazioni dettagliate sul processo di scansione registrato, sul target di scansione, le minacce individuate e le azioni intraprese su queste minacce.

17.3. Oggetti esclusi dalla scansione

Ci sono dei casi in cui si può avere bisogno di escludere certi file dalla scansione. Ad esempio, si può volere escludere un file di testo EISCAR dalla scansione all'accesso, oppure i file `.avi` dalla scansione a richiesta.

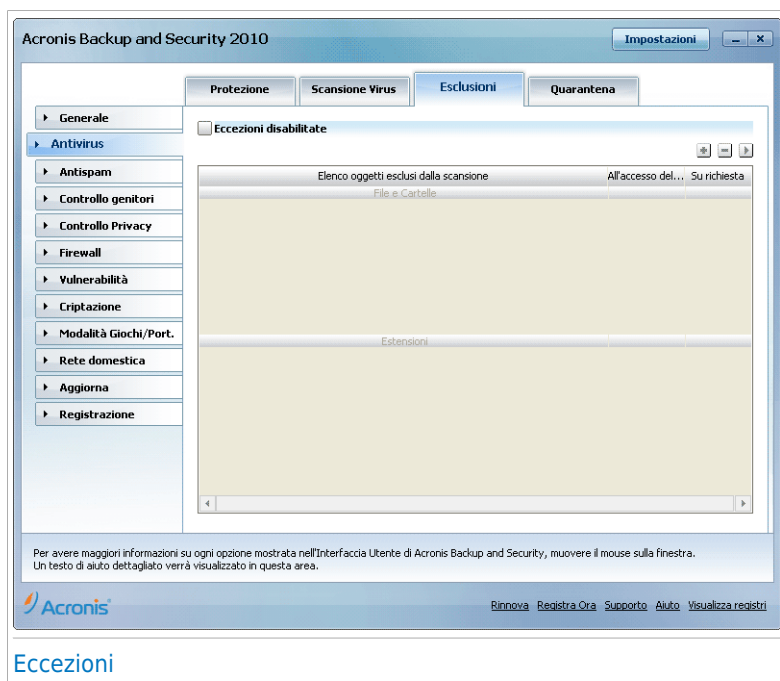
Acronis Backup and Security 2010 permette di escludere oggetti dalle scansioni all'accesso ed a richiesta, o da entrambi. Questa caratteristica cerca di ridurre i tempi di scansione e di evitare le interferenze con il vostro lavoro.

Due tipi di oggetti possono essere esclusi dalla scansione:

- **Percorsi** - Il file o cartella (inclusi tutti gli oggetti che essi contiene) indicato da un percorso specifico verrà escluso dalla scansione.
- **Estensioni** - tutti i file che hanno una specifica estensione verranno esclusi dalla scansione.

Nota

Gli oggetti esclusi dalla scansione all'accesso non verranno esaminati, non importa se sono visitati da voi o da un'applicazione.

Per visualizzare e gestire gli oggetti esclusi dalla scansione, fare clic su **Antivirus>Eccezioni** in Modalità Avanzata.

Eccezioni

Si possono visualizzare gli oggetti (file, cartelle, estensioni) esclusi dalla scansione. Potete vedere se ogni oggetto è stato escluso dalla scansione all'accesso, dalla scansione a richiesta o da entrambi.

Nota

Le eccezioni qui specificate NON verranno applicate nella scansione contestuale. La scansione contestuale è un tipo di scansione su richiesta: fare clic con il pulsante destro sul file o cartella che si vuole scansionare e selezionare **Scansiona con Acronis Backup and Security**.

Per rimuovere una voce dalla tabella, selezionarla e fare clic sul pulsante **Elimina**.

Per modificare una voce dalla tabella, selezionarla e fare clic sul pulsante **Modifica**. Apparirà una nuova finestra dove si potrà modificare l'estensione od il percorso da escludere ed il tipo di scansione dal quale escluderlo, a seconda delle necessità. Apportare le necessarie modifiche e cliccare **OK**.

Nota

È inoltre possibile fare clic con il pulsante destro sull'oggetto ed utilizzare le opzioni del menu di scelta rapida per modificarlo o eliminarlo.

Potete cliccare su **Ignorare** per ritornare alla situazione precedente alle modifiche effettuate alla tabella delle regole, sempre che non le abbiate salvate cliccando su **Applicare**.

17.3.1. Esclusione dei Percorsi dalla Scansione

Per escludere dei percorsi dalla scansione, fare clic sul pulsante **Aggiungi**. Verrete guidati dall'assistente di configurazione attraverso il processo di esclusione dei percorsi dalla scansione.

Passo 1/4 – Selezionare tipo di oggetto

Tipo di Oggetto.

Selezionare l'opzione di escludere un percorso dalla scansione.

Selezionare **Avanti**.

Passo 2/4 – Specificare i percorsi esclusi

Percorsi Esclusi

Per specificare i percorsi da escludere dalla scansione, utilizzare uno dei seguenti metodi:

- Cliccare **Sfoglia**, selezionare il file o cartella che volete venga escluso dalla scansione e quindi cliccare su **Aggiungere**.
- Scrivere il percorso che volete venga escluso dalla scansione nel campo modifica e cliccare **Aggiungere**.

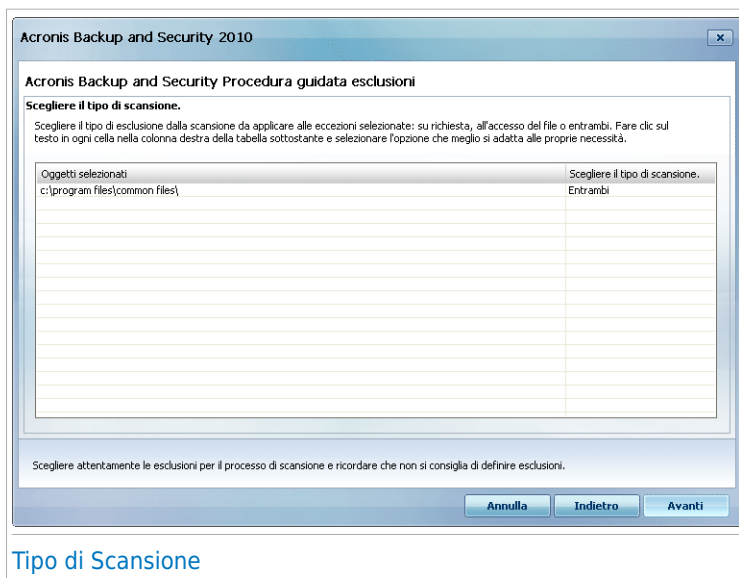
Nota

Se il percorso inserito non esiste, comparirà un messaggio di errore. Cliccare **OK** e controllare la validità del percorso.

I percorsi appariranno nella tabella man mano che vengono aggiunti. Potete aggiungere quanti percorsi volete.

Per rimuovere una voce dalla tabella, selezionarla e fare clic sul pulsante ⊟ **Elimina**.

Selezionare **Avanti**.

Passo 3/4 – Selezionare tipo di scansione

Tipo di Scansione

Potete vedere una tabella contenente i percorsi da escludere dalla scansione ed il tipo di scansione dal quale vengono esclusi.

Per default i percorsi selezionati verranno esclusi da entrambe le scansioni, all'accesso ed a richiesta. Per modificare quando applicare l'eccezione, cliccare nella colonna di destra e selezionare dall'elenco l'opzione desiderata.

Selezionare **Avanti**.

Passo 4/4 – Esaminare i file esclusi

Scansione dei File Esclusi

E' altamente consigliato esaminare i file nei percorsi specificati per essere sicuri che non siano infetti. Selezionare l'opzione di escludere un percorso dalla scansione.

Selezionare **Termina**.

17.3.2. Esclusione delle Estensioni dalla Scansione

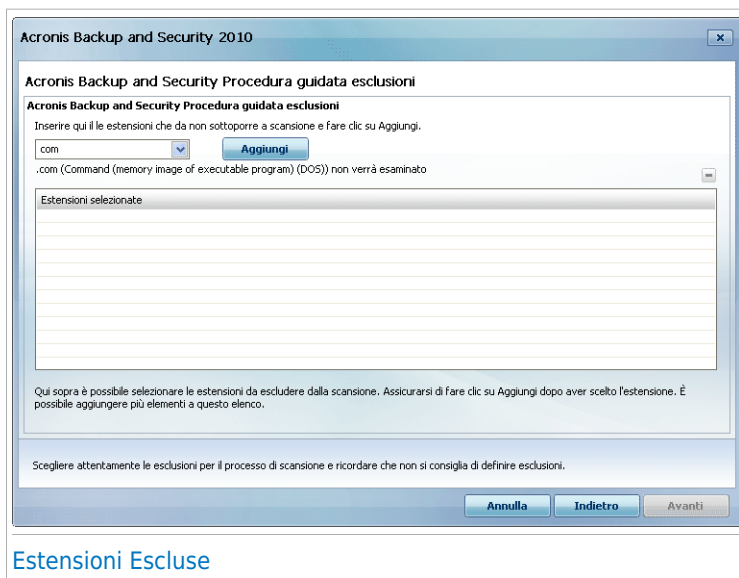
Per escludere delle estensioni dalla scansione, fare clic sul pulsante **Aggiungi**. Verrete guidati dall'assistente di configurazione attraverso il processo di esclusione delle estensioni dalla scansione.

Passo 1/4 – Selezionare tipo di oggetto

Tipo di Oggetto.

Selezionare l'opzione di escludere estensioni dalla scansione.

Selezionare **Avanti**.

Passo 2/4 – Specificare le estensioni escluse

Estensioni Escluse

Per specificare le estensioni da escludere dalla scansione, utilizzare uno dei seguenti metodi:

- Selezionare dal menu l'estensione che volete venga esclusa dalla scansione e quindi cliccare su **Aggiungere**.

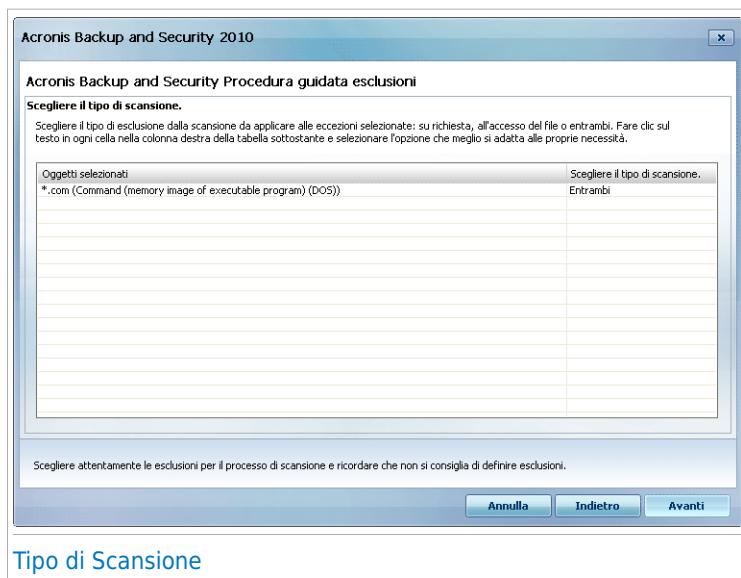
Nota
Il menu contiene un elenco di tutte le estensioni registrate sul vostro sistema. Quando selezionate un'estensione, potrete vedere la sua descrizione, se disponibile.

- Scrivere l'estensione che volete venga esclusa dalla scansione nel campo modifica e cliccare **Aggiungere**.

Le estensioni appariranno nella tabella man mano che vengono aggiunte. Potete aggiungere quante estensioni volete.

Per rimuovere una voce dalla tabella, selezionarla e fare clic sul pulsante ⊟ **Elimina**.

Selezionare **Avanti**.

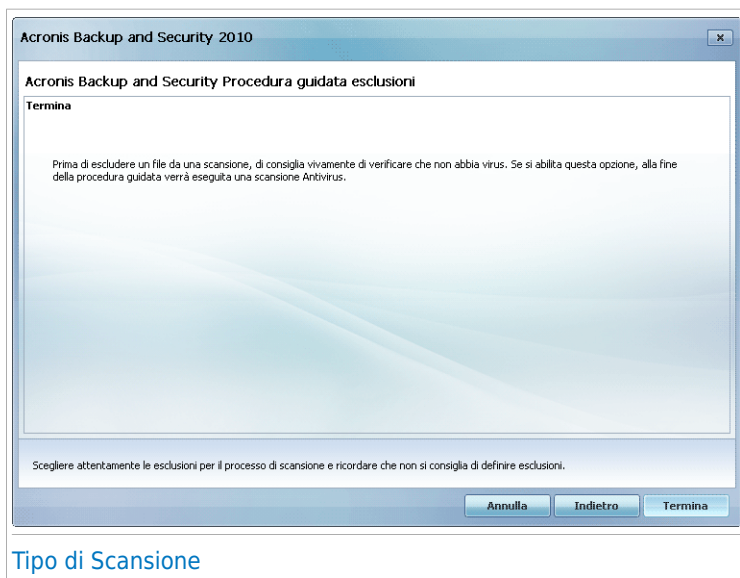
Passo 3/4 – Selezionare tipo di scansione

Tipo di Scansione

Potete vedere una tabella contenente le estensioni da escludere dalla scansione ed il tipo di scansione dal quale vengono escluse.

Per default le estensioni selezionate verranno escluse da entrambe le scansioni, all'accesso ed a richiesta. Per modificare quando applicare l'eccezione, cliccare nella colonna di destra e selezionare dall'elenco l'opzione desiderata.

Selezionare **Avanti**.

Passo 4/4 – Selezionare tipo di scansione

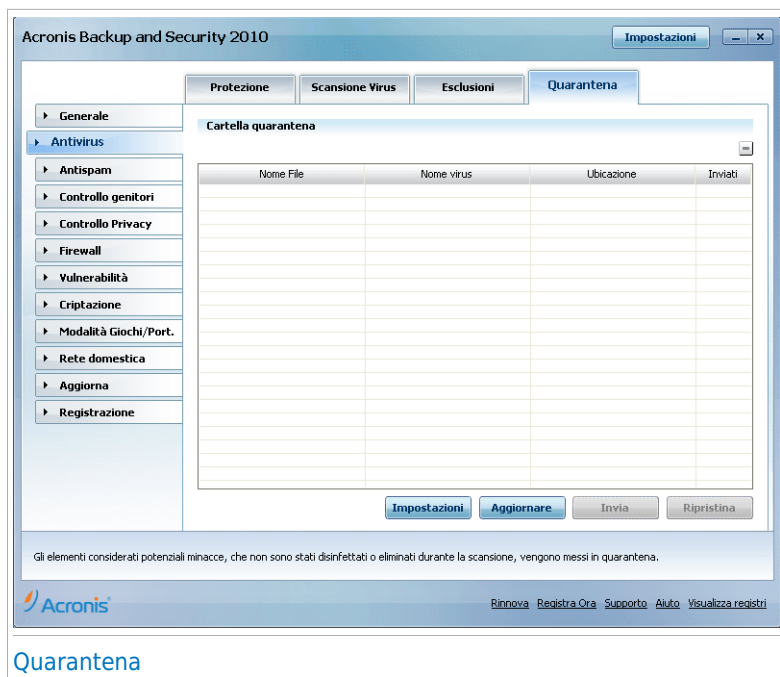
Tipo di Scansione

E' altamente consigliato esaminare i file con le estensioni specificate per essere sicuri che non siano infetti.

Selezionare **Termina**.

17.4. Area di Quarantena

Acronis Backup and Security 2010 consente di isolare i file infetti o sospetti in un'area sicura, chiamata quarantena. Isolando questi file in quarantena, scompare il rischio di essere infettati e contemporaneamente si ha la possibilità di inviare questi file ai Laboratori Acronis per ulteriori analisi.

Inoltre Acronis Backup and Security 2010 scansiona i file in quarantena dopo ogni aggiornamento di firme malware. I file puliti vengono spostati automaticamente alla loro ubicazione originale.

Per visualizzare e gestire i file in quarantena e per configurare le impostazioni della quarantena, fare clic su **Antivirus>Quarantena** in Modalità Avanzata.

Quarantena

La sezione Quarantena mostra tutti i file attualmente isolati nella cartella Quarantena. Per ogni file in quarantena, potete vedere il suo nome, il nome del virus rilevato, il percorso alla sua posizione originale e la data di invio.

Nota
Quando un virus è in quarantena, non può più arrecare alcun danno in quanto non può essere eseguito o letto.

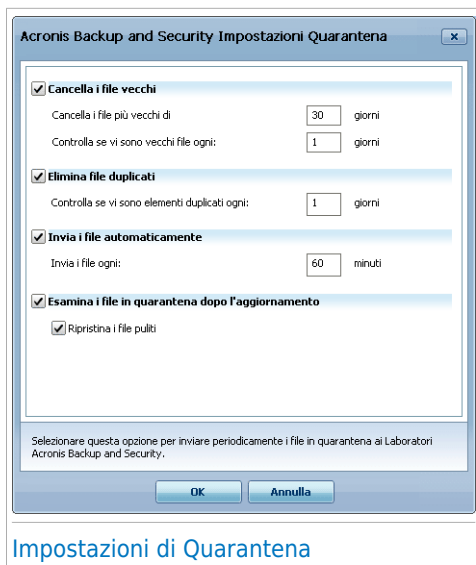
17.4.1. Gestione dei File in Quarantena

Potete inviare qualsiasi file selzionato dalla quarantena al lab Acronis cliccando su **Invia**. Per default, Acronis Backup and Security 2010 invierà automaticamente i file in quarantena ogni 60 minuti.

Per cancellare un file selezionato dalla quarantena, fare clic sul pulsante **Elimina**. Se si desidera inviare un file selezionato alla sua ubicazione originale, fare clic su **Ripristina**.

Menù contestuale. E' disponibile un menu contestuale che vi permette di gestire facilmente i file in quarantena. Sono disponibili le stesse opzioni su menzionate. Potete anche selezionare **Aggiornare** per aggiornare la sezione di Quarantena.

17.4.2. Configurazione delle Impostazioni di Quarantena

Per configurare le impostazioni di quarantena, cliccare su **Impostazioni**. Apparirà una nuova finestra.

Impostazioni di Quarantena

Utilizzando le impostazioni di quarantena, potete configurare Acronis Backup and Security 2010 per eseguire automaticamente le seguenti azioni:

Eliminare i vecchi file. Per eliminare automaticamente i vecchi file, selezionare l'opzione corrispondente. Dovete specificare il numero di giorni dopo i quali i file in quarantena devono essere eliminati e la frequenza con cui Acronis Backup and Security 2010 deve effettuare il controllo dei vecchi file.

Nota
Per default, Acronis Backup and Security 2010 effettuerà il controllo dei vecchi file ogni giorno ed eliminerà i file più vecchi di 30 giorni.

Elimina file duplicati. Per eliminare automaticamente i file duplicati in quarantena, selezionare l'opzione corrispondente. Dovete specificare il numero di giorni tra due controlli consecutivi dei duplicati.

Nota
Per default, Acronis Backup and Security 2010 effettuerà il controllo dei file duplicati in quarantena ogni giorno.

Invio automatico dei file. Per inviare automaticamente i file in quarantena, selezionare l'opzione corrispondente. Dovete specificare la frequenza con cui inviare i file.

Nota

Per default, Acronis Backup and Security 2010 invierà automaticamente i file in quarantena ogni 60 minuti.

Esaminare i file in quarantena dopo l'aggiornamento. Per esaminare automaticamente i file in quarantena dopo l'aggiornamento, selezionare l'opzione corrispondente. Potete scegliere di far tornare automaticamente i file puliti alla loro posizione originale selezionando **Ripristinare file puliti**.

Selezionare **OK** per salvare le modifiche e chiudere la finestra.

18. Antispam

Antispam Acronis impiega notevoli innovazioni tecnologiche e filtri standard dell'industria antispam per eliminare lo spam prima che raggiunga l'Inbox dell'utente.

18.1. Approfondimenti Antispam

Lo Spam rappresenta un problema in continua crescita, sia per i privati che per le aziende. Non è piacevole, non vorreste che i vostri figli lo vedessero, potrebbe penalizzarvi (per aver sprecato troppo tempo o per aver ricevuto mail pornografiche in ufficio) e non potete impedire alla gente di inviarlo. La miglior cosa da fare, ovviamente, e di fermarne la ricezione. Sfortunatamente lo Spam si presenta sotto molte forme e dimensioni e ce n'è veramente tanto in giro.

18.1.1. Filtri Antispam

Il Motore Antispam Acronis Backup and Security 2010 incorpora diversi filtri che assicurano l'assenza di SPAM nella vostra Inbox: Elenco amici, Elenco Spammers, Filtro Carattere, Filtro Immagine, Filtro URL, Filtro NeuNet (Heuristico) e Filtro Bayesiano.

Nota
E' possibile attivare/disattivare ognuno di questi filtri nel modulo **Antispam**, sezione Impostazioni.

Elenco Amici / Elenco Spammer

La maggior parte delle persone comunica regolarmente con un gruppo di persone o riceve messaggi da organizzazioni o società nello stesso dominio. Utilizzando **L'elenco Amici o Spammer**, potrete facilmente classificare da quali persone volete ricevere e-mail (Amici) indipendentemente dal contenuto del messaggio, o da quali persone non volete più ricevere nulla (spammer).

E' possibile gestire l'elenco Amici / Spammer dalla Modalità Avanzata oppure dalla Barra degli strumenti Antispam integrata in alcuni dei client di posta più comunemente usati.

Nota
Raccomandiamo di aggiungere i nomi dei vostri amici e gli indirizzi e-mail all'**elenco Amici**. Acronis Backup and Security 2010 non blocca i messaggi di coloro che sono nell'elenco; aggiungere amici aiuta a garantire che i messaggi leciti vengano recapitati.

Filtro Carattere

La maggior parte dei messaggi Spam sono scritti in caratteri cirillici e/o asiatici. Il filtro Carattere rileva questo tipo di messaggi e li etichetta come SPAM.

Filtro Immagine

Da quando l'eliminazione della scansione con il Filtro Euristico è diventata una scoperta, oggigiorno le cartelle di posta in arrivo sono piene di molti messaggi contenenti solo un immagine con contenuti insoliti. Per contrastare questo crescente problema, il **Filtro Immagine** confronta le firme delle immagine delle e-mail con il database di Acronis Backup and Security 2010. In caso di riconoscimento, l'email verrà etichettata come Spam.

Filtro URL

La maggior parte dei messaggi Spam contiene links a vari siti web. Questi siti solitamente contengono ulteriore pubblicità e la possibilità di acquistare oggetti e, alle volte, vengono usati per phishing.

Acronis mantiene un database di tali links. Il filtro URL esamina ogni link URL contenuto in un messaggio con il suo database. Se corrisponde, il messaggio viene etichettato come SPAM.

Filtro Euristico

Il **Filtro Euristico** esegue una serie di test a tutte le componenti del messaggio (ovvero, non solo l'intestazione ma anche il corpo del messaggio sia in formato HTML che di testo), alla ricerca di parole, frasi, links o altri elementi caratteristici dello SPAM. Basandosi sui risultati dell'analisi, esso aggiunge un punteggio SPAM al messaggio.

Il filtro rileva inoltre messaggi segnati come `ESPLICITAMENTE SESSUALE:` nell'oggetto e li etichetta come SPAM.

Nota

A partire dal 19 Maggio 2004 lo Spam contenente materiale a sfondo sessuale deve includere l'avviso `SEXUALLY-EXPLICIT` nell'oggetto, diversamente sarà passibile di sanzioni per violazione della legge federale.

Filtro Bayesiano

Il modulo **Filtro Bayesiano** classifica i messaggi secondo informazioni statistiche relative alla frequenza di specifiche parole contenute nei messaggi classificati come Spam in confronto a quelli dichiarati come non-Spam (da voi o dal filtro euristico).

Ciò significa, ad esempio, che se una determinata parola di quattro lettere appare più spesso in uno Spam, è naturale desumere che esiste una notevole possibilità che il successivo messaggio in entrata contenente la stessa parola SIA Spam. Vengono prese in considerazione tutte le parole rilevanti all'interno di un messaggio. Sintetizzando le informazioni statistiche, viene valutata la probabilità globale che l'intero messaggio sia Spam.

Questo modulo presenta un'altra interessante caratteristica: lo si può "addestrare". Si adatta velocemente alla tipologia di messaggi ricevuti da un determinato utente e immagazzina informazioni su tutto. Per funzionare efficacemente, il filtro va addestrato, ovvero gli vanno presentati esempi di Spam e di messaggi leciti, proprio come si addestra un cane a rilevare determinati odori. A volte il filtro va anche corretto – stimolato a correggersi quando prende una decisione sbagliata.

Importante

È possibile correggere il filtro bayesiano utilizzando i pulsanti **È spam** e **Non è spam** dalla Barra degli strumenti Antispam .

18.1.2. Operazione Antispam

Il motore Antispam Acronis Backup and Security 2010 usa tutti i filtri antispam combinati per determinare se un certo messaggio e-mail dovrebbe giungere alla **Posta in arrivo** o no.

Importante

I messaggi spam rilevati da Acronis Backup and Security 2010 sono marcati con il prefisso [SPAM] nell'oggetto. Acronis Backup and Security 2010 sposta automaticamente messaggi spam ad una cartella specifica, come segue:

- In Microsoft Outlook, i messaggi spam sono spostati nella cartella **Spam**, situata nella cartella **Posta eliminata**. La cartella **Spam** è creata durante l'installazione di Acronis Backup and Security 2010.
- In Outlook Express e Windows Mail, i messaggi spam sono spostati direttamente nella cartella **Posta eliminata**.
- In Mozilla Thunderbird, i messaggi spam sono spostati nella cartella **Spam**, situata nella cartella **Cestino**. La cartella **Spam** è creata durante l'installazione di Acronis Backup and Security 2010.

Se si utilizza un altro client per la posta, è necessario creare una regola per spostare i messaggi e-mail segnati come [SPAM] da Acronis Backup and Security 2010 in una cartella personalizzata di quarantena.

Ogni e-mail che arriva da Internet viene prima controllata con il filtro Elenco Amici/Elenco Spammer. Se l'indirizzo del mittente viene trovato nell'Elenco Spammer l'e-mail viene spostata direttamente nella vostra **Inbox**.

Diversamente, il filtro Elenco Spammer prenderà in carico l'e-mail per verificare se l'indirizzo del mittente è contenuto nel suo elenco. L'e-mail verrà contrassegnata come SPAM e spostata nella cartella **Spam** (situata in Microsoft Outlook) qualora il confronto con la lista abbia dato esito positivo.

Ancora, il filtro Carattere controllerà se l'e-mail è scritta con caratteri cirillici o asiatici. In questo caso l'e-mail verrà marcata come SPAM e spostata nella cartella **Spam**.

Qualora l'e-mail non fosse scritta con caratteri asiatici o cirillici, la stessa verrà passata al filtro Filtro Immagine. Il **Filtro Immagine** controllerà tutti I messaggi e-mail contenenti allegati con immagini con contenuti di spam.

Il filtro URL cercherà i link e li comparerà con i link del database di Acronis Backup and Security 2010. In caso di corrispondenza, il filtro aggiungerà un punteggio Spam alla e-mail.

Il Filtro Euristico prenderà in carico l'e-mail ed eseguirà una serie di test su tutte le componenti del messaggio, alla ricerca di parole, frasi, collegamenti o caratteristiche dello Spam. Il risultato sarà quello di aggiungere un altro punteggio Spam alla e-mail.

Nota

Se l'e-mail è marcata come SEXUALLY EXPLICIT nella riga del soggetto, Acronis Backup and Security 2010 la considererà come SPAM.

Il modulo del filtro Bayesiano analizzerà ulteriormente il messaggio, basandosi su informazioni statistiche relative all'incidenza con cui determinate parole appaiono nei messaggi classificati come Spam in paragone a quelli dichiarati come non-Spam (da voi o dal filtro euristico). Verrà aggiunto un punteggio Spam alla e-mail.

Se il risultato del punteggio (punteggio URL + punteggio Euristico + punteggio Bayesiano) eccede il punteggio Spam per un messaggio (impostato dall'utente nella sezione Antispam come livello di tolleranza), il messaggio viene considerato come SPAM.

18.1.3. Aggiornamenti Antispam

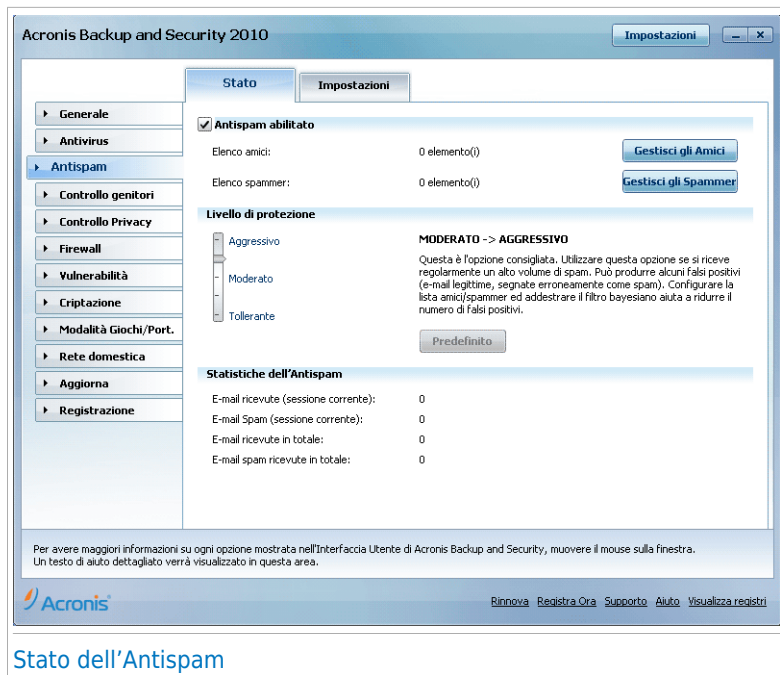
Ogni volta che esegui un aggiornamento:

- nuove impronte di immagini saranno aggiunte al **Filtro Immagine**.
- nuovi links verranno aggiunti al **Filtro URL**.
- nuove regole verranno aggiunte al **Filtro Euristico**.

Questo aiuterà ad incrementare l'effettività del tuo motore Antispam.

Per proteggerti contro gli spammers, Acronis Backup and Security 2010 può effettuareaggiornamenti automatici. Mantenere l'opzione di **Aggiornamento Automatico** attivata.

18.2. Stato

Per configurare la protezione Antispam, fare clic su **Antispam>Stato** in Modalità Avanzata.

Stato dell'Antispam

Potete vedere se l'Antispam è abilitato o disabilitato. Se desiderate cambiare lo stato dell'Antispam, deselezionare o selezionare la casella corrispondente.

Importante

Per impedire che lo Spam entri nella vostra **Inbox**, mantenere abilitato il **Antispam filter**.

Nella sezione **Statistiche** è possibile visionare i risultati della attività dell'Antispam presentati per sessione (da quando avete avviato il computer), oppure un riassunto (dall'installazione di Acronis Backup and Security 2010).

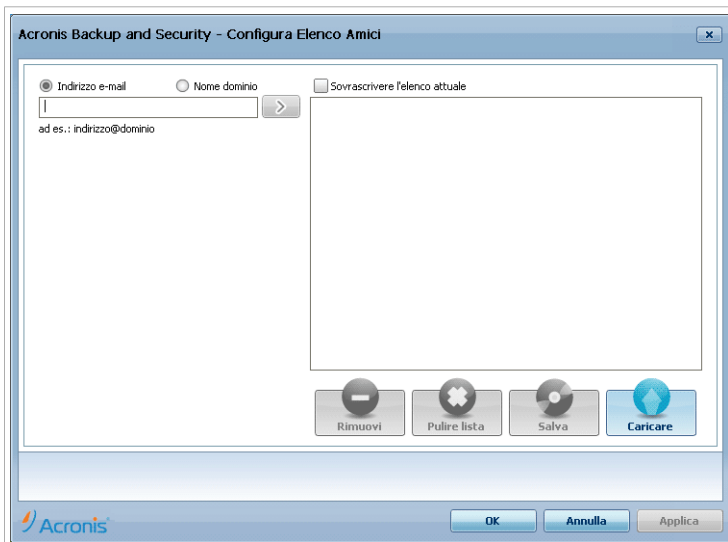
18.2.1. Impostazione del Livello di Protezione

Potete scegliere il livello di protezione che meglio si adatta alle vostre necessità di sicurezza. Trascinate il pulsante sulla barra per impostare il livello di protezione appropriato.

Ci sono 5 livelli di protezione:

Livello di protezione	Descrizione
Permissiva	Offre protezione per gli account che ricevono molta posta commerciale legittima. Il filtro lasciare passare la maggior parte delle e-mail, ma potrebbe produrre dei falsi negativi (spam classificato come mail legittime).
Permissivo a Moderato	Offre protezione per account che ricevono alcune mail commerciali legittime. Il filtro lasciare passare la maggior parte delle e-mail, ma potrebbe produrre dei falsi negativi (spam classificato come mail legittime).
Moderato	Offre protezione per account normali. Il filtro bloccherà la maggior parte dello spam, evitando al contempo i falsi positivi.
Da Moderato ad Aggressivo	Offre protezione per gli account che ricevono regolarmente ampi volumi di spam. Il filtro lascerà passare pochissimo spam, ma potrebbe produrre dei falsi positivi (mail legittime etichettate erroneamente come spam). Configura gli **Elenchi Amici/Spammer** e addestra il **Motore di Apprendimento (Bayesiano)** per ridurre il numero di falsi positivi.
Aggressiva	Offre protezione per gli account che ricevono regolarmente volumi di spam molto ampi. Il filtro lascerà passare pochissimo spam, ma potrebbe produrre dei falsi positivi (mail legittime etichettate erroneamente come spam). Aggiungete i vostri contatti alla **Lista Amici** per ridurre il numero di falsi positivi.

Per impostare il livello di protezine di default (**Da Moderato ad Aggressivo**) cliccare su **Livello di Default**.

18.2.2. Configurazione dell'Elenco Amici

L'**Elenco Amici** è l'elenco di tutti gli indirizzi email dai quali volete sempre ricevere messaggi, indipendentemente dal loro contenuto. I messaggi provenienti dai vostri amici non verranno etichettati come spam, anche se il loro contenuto potrebbe assomigliare allo Spam.

Nota

Qualsiasi mail in arrivo da un indirizzo contenuto nella lista **Elenco Amici**, sarà automaticamente consegnato alla vostra Inbox senza alcun ulteriore processo.

Per configurare l'Elenco Amici, fare clic su **Gestione Amici** (oppure fare clic sul pulsante **Amici** nella barra degli strumenti Antispam).

Elenco Amici

Qui potrete aggiungere o rimuovere elementi dall’**Elenco Amici**.

Se si desidera aggiungere un indirizzo email, selezionare il campo **Indirizzo E-mail**, inserire l’indirizzo e premere il pulsante ⊡. L’indirizzo apparirà nell’**Elenco amici**.

Importante

Sintassi: name@domain.com.

Se desiderate aggiungere un dominio, selezionare l' opzione **Dominio**, digitare dominio e premere il pulsante ⊡. Il dominio apparirà sull’**Elenco Amici**.

Importante

Sintassi:

- @domain.com, *domain.com e domain.com - tutte le mail provenienti da domain.com raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;
- *domain* - tutte le mail provenienti da domain (non importa il suffisso del dominio) raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;
- *com - tutte le mail con il suffisso di dominio com raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;

Per rimuovere un elemento dall'elenco, selezionarlo e fare clic su **Rimuovi**. Per eliminare tutti gli elementi dall'elenco fare clic su **Pulisci elenco** e quindi su **Sì** per confermare.

E' possibile salvare l'elenco Amici in un file in modo da poterlo riutilizzare su un altro computer o dopo aver reinstallato il prodotto. Per salvare l'elenco Amici, fare clic sul pulsante **Salva** e salvare nella posizione desiderata. Il file avrà estensione `.bwl`.

Per caricare un elenco Amici precedentemente salvato, fare clic sul pulsante **Carica** e aprire il corrispondente file `.bwl`. Per ripristinare il contenuto dell'elenco esistente quando si carica un elenco precedentemente salvato, selezionare **Sovrascrivi l'elenco attuale**.

Nota

Raccomandiamo di aggiungere i nomi dei vostri amici e gli indirizzi e-mail all'**elenco Amici**. Acronis Backup and Security 2010 non blocca i messaggi di coloro che sono nell'elenco; aggiungere amici aiuta a garantire che i messaggi leciti vengano recapitati.

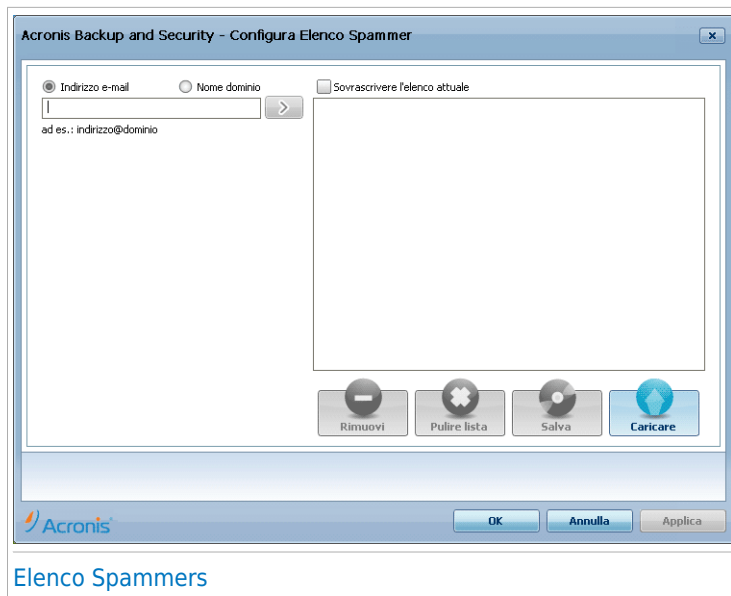
Selezionare **Applica** e **OK** per salvare & chiudere **l'Elenco Amici**.

18.2.3. Configurazione dell'Elenco Spammer

L'**Elenco Spammer** è l'elenco di tutti gli indirizzi e-mail dai quali non volete ricevere messaggi, indipendentemente dal loro contenuto.

Nota

Qualsiasi mail in arrivo da un indirizzo contenuto nell'**Elenco Spammer** verrà automaticamente marcato come Spam, senza alcun ulteriore processo.

Per configurare l'Elenco Spammer, fare clic su **Gestione Spammer** (oppure fare clic sul pulsante **Spammer** nella barra degli strumenti Antispam).

Elenco Spammers

Qui potrete aggiungere o rimuovere elementi dall’**Elenco Spammer**.

Se desiderate aggiungere un indirizzo email, selezionare il campo **Indirizzo Email**, inserire l’indirizzo e premere il pulsante ☒ . L’indirizzo apparirà nell’**Elenco Spammers**.

Importante

Sintassi: name@domain.com.

Se volete aggiungere un dominio, selezionare l'opzione **Dominio**, digitare il nome e fare un click su ☒. Il dominio apparirà nell’**Elenco Spammers**.

Importante

Sintassi:

- @domain.com, *domain.com e domain.com - tutte le mail provenienti da domain.com verranno marcate come Spam;
- *domain* - tutte le mail provenienti da domain (indipendentemente dai suffissi del dominio) verranno marcate come Spam;
- *com - tutte le mail con il suffisso di dominio com verranno marcate come Spam.

Avvertimento

Non aggiungere domini di servizi e-mail legittimi (ad esempio Yahoo, Gmail, Hotmail o altri) all'elenco Spammer. In caso contrario gli indirizzi e-mail ricevuti dagli utenti registrati di tali servizi verranno identificati come spam. Se ad esempio si aggiunge `yahoo.com` all'elenco Spammer, tutti i messaggi e-mail provenienti da indirizzi `yahoo.com` saranno contrassegnati come `[spam]`.

Per rimuovere un elemento dall'elenco, selezionarlo e fare clic su **Rimuovi**. Per eliminare tutti gli elementi dall'elenco fare clic su **Pulisci elenco** e quindi su **Sì** per confermare.

E' possibile salvare l'elenco Spammer in un file in modo da poterlo riutilizzare su un altro computer o dopo aver reinstallato il prodotto. Per salvare l'elenco Spammer, fare clic sul pulsante **Salva** e salvare nella posizione desiderata. Il file avrà estensione `.bwl`.

Per caricare un elenco Spammer precedentemente salvato, fare clic sul pulsante **Carica** e aprire il corrispondente file `.bwl`. Per ripristinare il contenuto dell'elenco esistente quando si carica un elenco precedentemente salvato, selezionare **Sovrascrivi l'elenco attuale**.

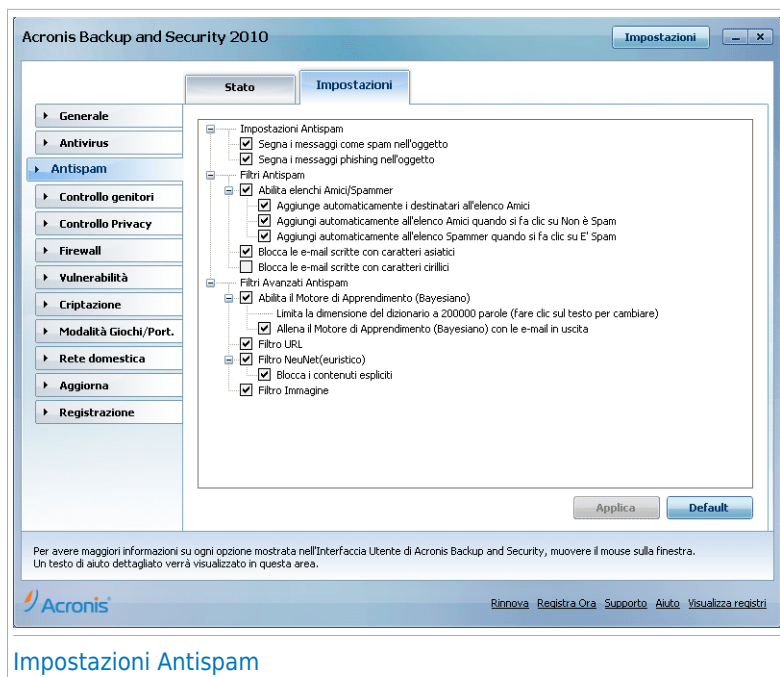
Selezionare **Applica** e **OK** tper salvare & chiudere **l'Elenco Spammer**.

Importante

Se si desidera installare nuovamente Acronis Backup and Security 2010, consigliamo prima di salvare gli elenchi **Amici** / **Spammer** e di ricaricarli al termine del processo di re-installazione.

18.3. Impostazioni

Per configurare le impostazioni ed i filtri antispam, fare clic su **Antispam>Impostazioni** in Modalità Avanzata.

Impostazioni Antispam

Sono disponibili tre categorie di opzioni (**Impostazioni Antispam**, **Filtri Antispam** and **Filtri Avanzati Antispam**) organizzati come menu espandibili, simili a quelli di Windows.

Nota
Selezionare una casella con "+" per aprire una categoria oppure una casella con "-" per chiudere una categoria.

Per attivare/disattivare una opzione, selezionare/pulire il checkbox corrispondente.

Per applicare le impostazioni predefinite, cliccare su **Default**.

Click **Applica** per salvare le modifiche.

18.3.1. Impostazioni Antispam

- **Contrassegna i messagi spam nel soggetto** - tutti i messaggi email considerati come Spam verranno marcati con Spam nel soggetto.
- **Marca l'oggetto dei messagi considerati come phishing** - tutte le mail considerate messaggi di phishing saranno etichettate come SPAM sulla linea di Oggetto.

18.3.2. Filtri Antispam

- **Abilita elenchi Amici / Spammer** - filtra i messaggi e-mail utilizzando gli Elenchi Amici/Spammer.
  - **Aggiungi automaticamente all'elenco degli Amici** - aggiunge automaticamente i mittenti all'Elenco Amici.
  - **Aggiungi Automaticamente all'Elenco Amici** - quando verrà premuto il pulsante **Non è Spam** dalla Barra degli strumenti Antispam, il mittente della e-mail selezionata verrà aggiunto automaticamente all'Elenco Amici.
  - **Aggiungi automaticamente all'elenco Spammer** - quando verrà premuto il pulsante **È Spam** dalla Barra degli strumenti Antispam il mittente della e-mail selezionata verrà automaticamente aggiunto all'Elenco Spammer.

Nota
I tasti **Non è Spam** ed **è Spam** vengono utilizzati per "istruire" il Filtro bayesiano.

- **Bloccare messaggi e-mail scritti in caratteri asiatici** - blocca i messaggi scritti in Caratteri Asiatici.
- **Bloccare messaggi e-mail scritti in caratteri cirillici** - blocca i messaggi scritti in Caratteri cirillici.

18.3.3. Filtri Avanzati Antispam

- **Abilita il motore di Apprendimento (bayesiano)** - attiva/disattiva il Motore di Apprendimento (bayesiano).
  - **Limita la dimensione del vocabolario a 200000 parole** - con questa opzione potete impostare la dimensione del dizionario Bayesiano – se minore è più veloce, se maggiore è più accurato.

Nota
La dimensione consigliata è: 200.000 parole.

  - **Istruisci il Motore di Apprendimento (bayesiano) per le e-mails in uscita** - istruisce il Motore di Apprendimento (bayesiano) per le e-mail in uscita.
- **Filtro URL** - attiva/disattiva il Filtro URL;
- **Filtro Euristico** - attiva/disattiva il Filtro Euristico;
  - **Blocco dei contenuti espliciti** - attiva/disattiva la scansione di messaggi "SESSUALMENTE ESPLICITO" nell'oggetto.
- **Filtro immagini** - attivare/disattivare il Filtro immagini.

19. Controllo genitori

Il Controllo dei Genitori vi permette di controllare l'accesso ad Internet e ad applicazioni specifiche di ogni utente che possieda un account nel sistema.

Potete configurare il Controllo dei Genitori per bloccare:

- pagine web inappropriate.
- accesso ad Internet, durante specifici periodi di tempo (come durante le ore di studio).
- pagine web, e-mail e messaggi istantanei contenenti determinate parole.
- applicazioni come giochi, chat, programmi di condivisione di file ed altri.
- messaggi istantanei inviati da contatti chat diversi da quelli consentiti.

Importante

Solo gli utenti con diritti di amministrazione (amministratori del sistema) possono accedere e configurare il Controllo dei Genitori. Per essere sicuri che solo voi potrete modificare le impostazioni del Controllo dei Genitori per qualsiasi utente, potete proteggerle mediante una password. Vi verrà chiesto di configurare la password quando abiliterete il Controllo dei Genitori per un utente specifico.

Per utilizzare con successo il Controllo dei Genitori e limitare l'uso del computer e le attività online dei vostri bambini, dovete completare questi task:

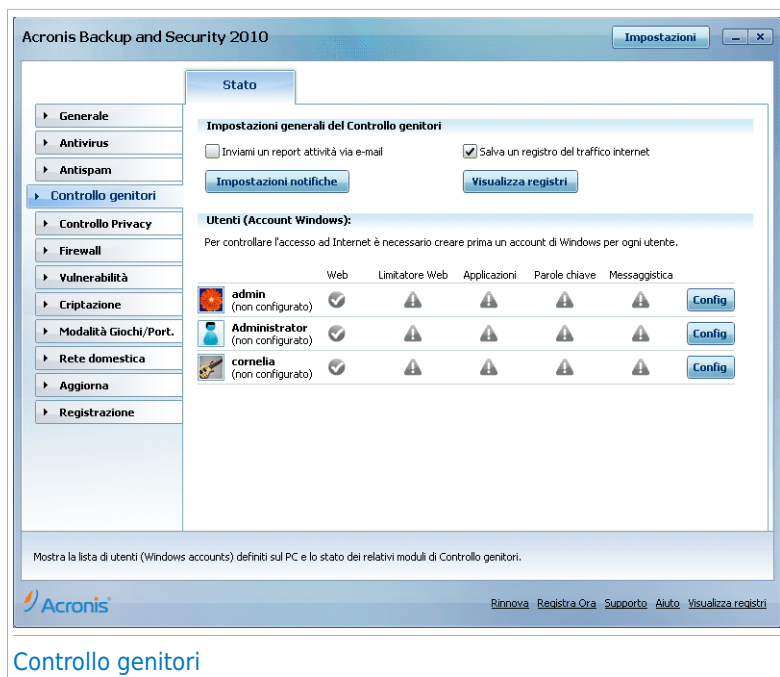
1. Creare degli account di Windows limitati (standard) per i bambini.

Nota

Per imparare a creare account di Windows, fare clic su Guida in linea e Supporto tecnico di Windows (nel menu Start, fare clic su **Guida in linea e Supporto tecnico**).

2. Configurare il Controllo dei Genitori per gli account di Windows che verranno usati dai vostri bambini.

Per configurare il Controllo Genitori, fare clic su **Controllo Genitori** in Modalità Avanzata.

Controllo genitori

E' possibile visualizzare le informazioni relative allo stato del Controllo Genitori per ogni account utente di Windows. La categoria di età è elencata al di sotto di ciascun nome utente se il Controllo Genitori è abilitato. Se il Controllo Genitori è disabilitato, lo stato è **non configurato**.

Inoltre è possibile visualizzare lo stato di ciascuna caratteristica del Controllo Genitori per utente:

Cerchio verde con un segno di spunta: La caratteristica è abilitata.

Cerchio rosso con un punto esclamativo: La caratteristica è disabilitata.

Fare clic sul pulsante **Modifica** vicino ad un nome utente per aprire la finestra in cui è possibile configurare il Controllo Genitori per l'account utente corrispondente.

Le seguenti sezioni di questo capitolo presentano in dettaglio le funzioni del Controllo dei Genitori e come configurarle.

19.1. Configurazione del Controllo Genitori per un utente

Per configurare il Controllo Genitori per uno specifico account utente fare clic sul pulsante **Modifica** corrispondente a tale account utente e quindi fare clic sulla scheda **Stato**.

Stato del Controllo Genitori

Per configurare il Controllo dei Genitori per questo account, seguire questi passaggi:

1. Abilitare il Controllo Genitori per questo account utente selezionando la casella di controllo **Controllo Genitori**.

Importante

Mantenere il **Controllo dei Genitori** abilitato per proteggere i vostri bambini dai contenuti inopportuni utilizzando le vostre regole di accesso al computer personalizzate.

2. Impostare una password per proteggere le vostre impostazioni del Controllo dei Genitori. Per ulteriori informazioni, vi preghiamo di riferirvi a *«Protezione delle Impostazioni del Controllo dei Genitori»* (p. 179).
3. Impostare la categoria di età per permettere ai bambini di accedere solo ai siti web appropriati per la loro età. Per ulteriori informazioni fare riferimento a *«Impostazione della Categoria di Età»* (p. 180).
4. Configurare le opzioni di controllo per questo utente come necessario:
   - **Invia un rapporto attività via e-mail.** Viene inviata una notifica e-mail ogni volta che il Controllo Genitori di blocca un'attività di questo utente.
   - **Salva un registro del traffico Internet.** Registra i siti web visitati dall'utente.

Per ulteriori informazioni fare riferimento a *«Controllo Attività dei Bambini»* (p. 183).

5. Fare clic su un'icona o una scheda per configurare la caratteristica di Controllo Genitori corrispondente:
   - **Web** - per filtrare la navigazione sul web secondo le regole impostate nella sezione Web.
   - **Applicazioni** per bloccare l'accesso alle applicazioni specificate nella sezione Applicazioni.
   - **Parole Chiave** - per filtrare l'accesso al web, alla posta ed all'instant messaging secondo le regole impostate nella sezione Parole Chiave.
   - **IM** - per consentire o impedire le chat con i contatti di instant messaging secondo le regole impostate nella sezione Traffico IM.
   - **Limitatore di Tempo** - per consentire l'accesso al web secondo l'orario stabilito nella sezione Limitatore di Tempo.

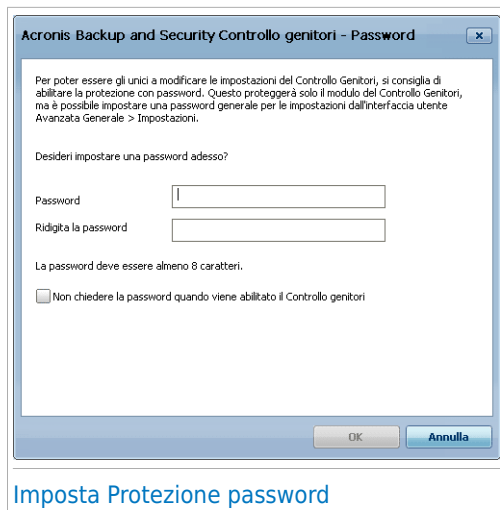
Nota

Per imparare a configurarle, vi preghiamo di riferirvi ai seguenti argomenti in questo capitolo.

Per bloccare completamente l'accesso ad internet, fare clic sul pulsante **Blocca Internet**.

19.1.1. Protezione delle Impostazioni del Controllo dei Genitori

Se non siete l'unica persona ad utilizzare questo computer con diritti di amministratore, consigliamo di proteggere le vostre Impostazioni del Controllo dei Genitori con una password. Impostando una password, impedirete ad altri utenti con diritti di amministratore di modificare le impostazioni del Controllo dei Genitori che avete configurato per un utente specifico.

Acronis Backup and Security 2010 vi chiederà di default di impostare una password quando abiliterete il Controllo dei Genitori.

Imposta Protezione password

Per impostare la protezione mediante password, fare come segue:

1. Digitare la password nel campo **Password**.
2. Digitare di nuovo la password nel campo **Ridigitare Password** per confermarla.
3. Selezionare **OK** per salvare la password e chiudere la finestra.

Una volta impostata la password, se desiderate modificare le impostazioni del Controllo dei Genitori, vi verrà richiesta la password. Gli altri amministratori del sistema (se ci fossero) dovranno anche fornire la password per potere modificare le impostazioni del Controllo dei Genitori.

Nota

Questa password non proteggerà altre impostazioni di Acronis Backup and Security 2010.

Nel caso in cui non impostate una password e non volete che questa finestra compaia di nuovo, selezionare **Non chiedere password all'abilitazione del Controllo dei Genitori**.

19.1.2. Impostazione della Categoria di Età

Il Filtro Euristico Web analizza le pagine web e blocca quelle che corrispondono a modelli dal contenuto potenzialmente inappropriato.

Per filtrare l'accesso al web secondo regole predefinite basate sull'età, dovrete impostare un livello specifico di tolleranza. Trascinate il pulsante scorrevole lungo

la barra per impostare il livello di tolleranza che considerate appropriato per l'utente selezionato.

Ci sono 3 livelli di tolleranza:

Livello di tolleranza	Descrizione
Bambino	Offre un accesso web limitato, secondo le impostazioni raccomandate per gli utenti al di sotto dei 14 anni. Le pagine web con contenuto potenzialmente dannoso per i bambini (porno, sessualità, droghe, hacking ecc.) sono bloccate.
Adolescenti	Offre un accesso web limitato, secondo le impostazioni raccomandate per gli utenti con età tra i 14 e i 18 anni. Le pagine web con contenuto sessuale, pornografico o per adulti sono bloccate.
Adulti	Offre un accesso illimitato a tutte le pagine web indipendentemente dal loro contenuto.

Cliccare su **Livello di Default** per impostare il pulsante scorrevole al livello di default.

Se si desidera avere maggior controllo sul tipo di contenuto a cui l'utente è esposto su Internet, è possibile definire le categorie di contenuto web che verranno bloccate dal filtro web. Per selezionare che tipi di contenuto web si desidera bloccare, fare clic su **Categorie Personalizzate**. Apparirà una nuova finestra:

Categorie Filtri Web

Selezionare la casella di controllo corrispondente alla categoria che si desidera bloccare e all'utente non sarà più permesso l'accesso ai siti web corrispondenti a tale categoria. Per rendere la selezione più semplice, le categorie di contenuto web sono elencate in base al gruppo di età per cui potrebbero essere considerate appropriate:

- **Categorie Profilo Bambino** include contenuti a cui è consentito l'accesso a bambini al di sotto dei 14 anni.

Categoria	Descrizione
Giochi	Siti web che offrono giochi da browser, forum di discussione sui giochi, download di giochi, trucchi, soluzioni, ecc.
Video/Foto	Website che ospitano gallerie di video o foto.
IM	Applicazioni di messaggistica istantanea.
Motori di Ricerca	Motori e portali di ricerca.
TLD Regionale	Siti web il cui nome di dominio è al di fuori della regione dell'utente.
Notizie	Giornali on-line.

- **Categorie Profilo Adolescenti** include contenuti che possono essere considerati sicuri per bambini fra i 14 e i 18 anni di età.

Categoria	Descrizione
Blocco Proxy Web	Siti web utilizzati per mascherare l'URL di un sito web richiesto.
Tabloid	Riviste on-line.
Gioco d'Azzardo	Casino on-line, siti web di scommesse, siti che offrono consigli sulle scommesse, forum sulle scommesse, ecc.
Shopping Online	Negozi e boutique on-line.
Social Network	Siti web di Social Networking.

- **Categorie Profilo Adulto** include contenuti non adatti ai bambini o agli adolescenti.

Categoria	Descrizione
Pornografia	Siti web con contenuto pornografico.
Odio / Violenza / Razzismo / Droghe	Siti web con contenuto violento o razzista, che promuovono il terrorismo o l'utilizzo di droghe.
Medicinali / Alcool / Sigari	Siti web che vendono o pubblicizzano medicinali, alcool o prodotti a base di tabacco.
Attività Illegali	Siti web che promuovono la pirateria od ospitano contenuti pirata.
Pagamenti On-line	Moduli web per i pagamenti on-line e sezioni di pagamento dei negozi on-line. L'utente può visitare i negozi on-line ma i tentativi di acquisto vengono bloccati.
Appuntamenti On-line	Siti web per appuntamenti per adulti, con chat, video o scambio di foto.

Fare clic su **Applica** per salvare le categorie di contenuto web bloccato per l'utente.

19.2. Controllo Attività dei Bambini

Acronis Backup and Security 2010 permette di controllare ciò che fanno i vostri figli al computer anche quando non siete presenti. Possono essere inviati avvisi via e-mail ogni volta che il modulo Controllo Genitori blocca un'attività. Inoltre è possibile salvare un registro con la cronologia dei siti visitati.

Selezionare le opzioni che si desidera abilitare:

- **Invia un rapporto attività via e-mail.** Viene inviata una notifica e-mail ogni volta che il Controllo Genitori di blocca un'attività.
- **Salva un registro del traffico Internet.** Registra i siti web visitati dagli utenti per cui è abilitato il Controllo Genitori.

19.2.1. Controllo dei Siti Web visitati

Acronis Backup and Security 2010 registra per default i siti web visitati dai bambini.

Per visualizzare i registri fare clic su **Visualizza Registri** per aprire Cronologia&Eventi e selezionare **Registro Internet**.

19.2.2. Configurazione Notifiche E-mail

Per ricevere notifiche via e-mail quando il Controllo Genitori blocca un'attività, selezionare **Invia un rapporto attività via e-mail** nella finestra di configurazione generale del Controllo Genitori. Verrà richiesto di configurare le impostazioni dell'account e-mail. Fare clic su **Sì** per aprire la finestra di configurazione.

Nota

E' possibile aprire la finestra di configurazione in un secondo momento facendo clic su **Impostazioni Notifiche**.

Impostazioni E-mail

Le impostazioni dell'account e-mail devono essere configurate come segue:

- **Server SMTP in Uscita** - digitare l'indirizzo del server di posta utilizzato per inviare i messaggi e-mail.
- Se il server usa una porta diversa rispetto alla porta di default 25, digitare il numero della porta nel campo corrispondente.
- **Indirizzo e-mail mittente** - digitare l'indirizzo che si vuole che appaia nel campo **Da** dell'e-mail.
- **Indirizzo e-mail destinatario** - digitare l'indirizzo a cui si desidera inviare i rapporti.
- Se il server richiede l'autenticazione, selezionare la casella di controllo **Il mio server SMTP richiede l'autenticazione** e digitare il nome utente e la password nei campi corrispondenti.

Nota

Se non si conoscono tali impostazioni apprire l'applicazione usata per la posta e controllare le impostazioni dell'account e-mail.

Per convalidare la configurazione, fare clic sul pulsante **Verifica Impostazioni**. Se vengono identificati dei problemi durante la convalida, Acronis Backup and Security 2010 comunicherà quali aree necessitano della vostra attenzione.

Selezionare **OK** per salvare le modifiche e chiudere la finestra.

19.3. Controllo Web

Il **Controllo Web** vi aiuta a bloccare l’accesso ai siti web inappropriati. Una lista di utenti per bloccare sia i siti inappropriati che parte di essi é fornita e aggiornata da Acronis Backup and Security 2010 come parte del processo di aggiornamento regolare.

Per configurare il Controllo Web per uno specifico account utente fare clic sul pulsante **Modifica** corrispondente a tale account utente e quindi fare clic sulla scheda **Web**.

Controllo Web

Per abilitare questa protezione selezionare la casella di controllo che corrisponde a **Abilita il Controllo Web**.

19.3.1. Creazione Regole di Controllo Web

Per permettere o bloccare l'accesso ad un sito web seguire questi passi:

1. Fare clic su **Permetti Sito** oppure su **Blocca Sito**. Apparirà una nuova finestra:

Specificare i siti web

2. Inserire l'URL del sito web nel campo **Sito web**.
3. Selezionare l'azione desiderata per questa regola - **Permetti** oppure **Blocca**.
4. Cliccare su**OK** per aggiungere la regola.

19.3.2. Gestione delle Regole di Controllo Web

Le regole di Controllo Web configurate sono elencate in una tabella nella parte inferiore della finestra. Per ogni regola del Controllo Web sono elencati l'indirizzo del sito web e lo stato attuale.

Per modificare una regola, selezionarla e fare clic sul pulsante **Modifica** e quindi eseguire le modifiche necessarie nella finestra di configurazione. Per eliminare una regola, selezionarla e fare clic sul pulsante **Elimina**.

È anche necessario selezionare quale azione verrà intrapresa da Controllo Genitori di Acronis Backup and Security 2010 per i siti web per cui non esistono regole di Controllo Web:

- **Permetti tutti i siti, tranne quelli nell'elenco**. Selezionare questa opzione per permettere l'accesso a tutti i siti web eccetto quelli per cui è stata impostata l'azione **Blocca**.
- **Blocca tutti i siti, tranne quelli nell'elenco**. Selezionare questa opzione per bloccare l'accesso a tutti i siti web eccetto quelli per cui è stata impostata l'azione **Permetti**.

19.4. Limitatore di Tempo su Web

Il **Tempo limitato sul web** ti aiuta a bloccare l'accesso a internet per determinati periodi di tempo.

Nota

Acronis Backup and Security 2010 eseguirà aggiornamenti ogni ora indipendentemente dall'impostazione **Tempo limitato sul web**.

Per configurare il Limitatore di Orario Web per uno specifico account utente fare clic sul pulsante **Modifica** corrispondente a tale account utente e quindi fare clic sulla scheda **Limitatore Web**.

Limitatore di Tempo su Web

Per abilitare questa protezione seleziona la casella di controllo che corrisponde a **Abilita Tempo limitato sul web**.

Selezionare gli intervalli di tempo in cui tutti i collegamenti a Internet verranno bloccati. È possibile fare clic sulle celle individuali oppure fare clic e trascinare per coprire periodi di tempo più lunghi. Inoltre è anche possibile fare clic su **Blocca tutto** per selezionare tutte le celle e implicitamente bloccare completamente l'accesso web. Se si fa clic su **Permetti tutto**, le connessioni Internet saranno sempre permesse.

Importante

I box colorati in grigio rappresentano l'intervallo di tempo quando la connessione internet è bloccata.

19.5. Controllo applicazioni

Il **Controllo Applicazioni** ti aiuta a bloccare qualsiasi applicazione in esecuzione. Giochi, messaggi software, oltre ad altre categorie di software e minacce che in questo caso possono essere bloccati. Le applicazioni bloccate sono così protette da modifiche, e non possono essere copiate o spostate. È possibile bloccare le applicazioni permanentemente o solo per determinati periodi di tempo, ad esempio quando i vostri bambini dovrebbero fare i compiti.

Per configurare il Controllo Applicazioni per uno specifico account utente fare clic sul pulsante **Modifica** corrispondente a tale account utente e quindi fare clic sulla scheda **Applicazioni**.

Controllo applicazioni

Per abilitare questa protezione selezionare la casella di controllo che corrisponde a **Abilita Controllo Applicazioni**.

19.5.1. Creazione Regole di Controllo Applicazioni

Per bloccare o limitare l'accesso ad un'applicazione seguire questi passi:

1. Fare clic su **Blocca Applicazione** oppure su **Restringi Applicazione**. Apparirà una nuova finestra:

Specificare l'applicazione

2. Fare clic su **Sfoglia** per localizzare l'applicazione di cui si desidera bloccare/restringere l'accesso.
3. Selezionare l'azione della regola:
   - **Blocca permanentemente** per bloccare completamente l'accesso all'applicazione.
   - **Blocca in base ad un programma** per limitare l'accesso a determinati intervalli di tempo.

   Se si sceglie di restringere l'accesso piuttosto che bloccare completamente l'applicazione, è anche necessario selezionare dalla griglia i giorni e gli intervalli di tempo durante i quali l'accesso è bloccato. È possibile fare clic sulle celle individuali oppure fare clic e trascinare per coprire periodi di tempo più lunghi. Inoltre è anche possibile fare clic su **Seleziona tutto** per selezionare tutte le celle e implicitamente bloccare completamente l'applicazione. Se si fa clic su **Deseleziona tutto**, l'accesso all'applicazione sarà permesso in ogni momento.
4. Cliccare su**OK** per aggiungere la regola.

19.5.2. Gestione Regole di Controllo Applicazioni

Le regole di Controllo Applicazioni che sono state configurate sono elencate in una tabella nella parte inferiore della finestra. Per ogni regola di Controllo Applicazioni viene elencato il nome dell'applicazione, il percorso e lo stato attuale.

Per modificare una regola, selezionarla e fare clic sul pulsante **Modifica** e quindi eseguire le modifiche necessarie nella finestra di configurazione. Per eliminare una regola, selezionarla e fare clic sul pulsante **Elimina**.

19.6. Controllo parole chiave

Il Controllo Parole Chiave aiuta a bloccare l'accesso degli utenti a messaggi e-mail, pagine web e messaggi istantanei che contengano parole specifiche. Utilizzando il Controllo Parole Chiave è possibile impedire ai bambini di vedere parole o frasi inappropriate quando sono online.

Nota

Il Controllo Parole Chiave per la messaggistica istantanea è disponibile solo per Yahoo Messenger e Windows Live (MSN) Messenger.

Per configurare il Controllo Parole Chiave per uno specifico account utente fare clic sul pulsante **Modifica** corrispondente a tale account utente e quindi fare clic sulla scheda **Parole Chiave**.

Controllo parole chiave

Selezionare la casella di controllo **Abilita Controllo Parole Chiave** se si desidera usare questa funzione di controllo.

19.6.1. Creazione Regole di Controllo Parole Chiave

Per bloccare una parola o una frase è necessario seguire questi passi:

1. Fare clic su **Blocca Parola Chiave**. Apparirà una nuova finestra:

Specificare Parole Chiave

2. Digitare la parola o frase che si desidera bloccare nel campo di immissione. Se si desidera che vengano rilevate solo parole intere, selezionare la casella di controllo **Solo parole intere**.
3. Selezionare il tipo di traffico che Acronis Backup and Security 2010 dovrà analizzare alla ricerca della parola specificata.

Opzione	Descrizione
HTTP	Le pagine web che contengono la parola chiave sono bloccate.
POP3	I messaggi e-mail che contengono la parola chiave sono bloccati.
Instant Messaging	I messaggi istantanei che contengono la parola chiave sono bloccati.

4. Cliccare su**OK** per aggiungere la regola.

19.6.2. Gestione delle Regole di Controllo Parole Chiave

Le regole di Controllo Parole Chiave che sono state configurate sono elencate in una tabella nella parte inferiore della finestra. Per ogni regola di Controllo Parole Chiave vengono elencate le parole e lo stato attuale per i diversi tipi di traffico.

Per modificare una regola, selezionarla e fare clic sul pulsante ▶ **Modifica** e quindi eseguire le modifiche necessarie nella finestra di configurazione. Per eliminare una regola, selezionarla e fare clic sul pulsante ⊟ **Elimina**.

19.7. Controllo del Chat (IM)

Il Controllo del Chat vi permette di specificare i contatti chat con i quali ai vostri bambini è permesso chattare.

Nota

Il Controllo Chat si trova disponibile solo per Yahoo Messenger and Windows Live (MSN) Messenger.

Per configurare il Controllo IM per uno specifico account utente fare clic sul pulsante **Modifica** corrispondente a tale account utente e quindi fare clic sulla scheda **Messaggistica**.

Controllo Chat

Selezionare la casella **Abilitare il Controllo del Chat** se desiderate utilizzare questa funzione di controllo.

19.7.1. Creazione di regole di controllo della messaggistica istantanea (IM)

Per permettere o bloccare la messaggistica istantanea con un contatto, seguire questi passi:

1. Fare clic su **Blocca ID IM** oppure **Permetti ID IM**. Apparirà una nuova finestra:

Aggiungi contatto Chat

2. Digitare il nome del contatto nel campo **Nome**.
3. Digitare l'indirizzo e-mail o il nome utente utilizzato dal contatto IM nel campo **E-mail o ID IM**.
4. Scegliere il programma al quale è associato il contatto.
5. Selezionare l'azione per questa regola - **Blocca** oppure **Permetti**
6. Cliccare su**OK** per aggiungere la regola.

19.7.2. Gestione di regole di controllo della messaggistica istantanea (IM)

Le regole di Controllo IM configurate sono elencate in una tabella nella parte inferiore della finestra. Per ogni regola del Controllo IM sono elencati il nome, l'ID IM, l'applicazione IM e lo stato attuale.

Per modificare una regola, selezionarla e fare clic sul pulsante **Modifica** e quindi eseguire le modifiche necessarie nella finestra di configurazione. Per eliminare una regola, selezionarla e fare clic sul pulsante **Elimina**.

Si deve inoltre selezionare quale azione deve intraprendere il Controllo Genitori di Acronis Backup and Security 2010 per i contatti IM per i quali non è stata creata alcuna regola. Selezionare **Blocca** o **Permetti IM con tutti i contatti, tranne quelli nell'elenco**.

20. Controllo della Privacy

Acronis Backup and Security 2010 esegue il monitoraggio di dozzine di potenziali “hotspots” nel vostro sistema dove lo spyware potrebbe agire; inoltre analizza qualsiasi cambiamento avvenuto sia nel sistema che sul software. Le minacce dello spyware sono quindi bloccate in tempo reale. Il modulo è attivo e blocca Trojan o altri codici installati da hackers, nel tentativo di compromettere la vostra privacy inviando informazioni personali, quali numeri di carte di credito per esempio, dal vostro computer ad altri.

20.1. Statistiche Controllo Privacy

Per configurare il Controllo della Privacy e visualizzare informazioni riguardanti la sua attività, andare su **Controllo della Privacy>Stato** in Modalità Avanzata.

Statistiche Controllo Privacy

Potete vedere se il Controllo della Privacy è abilitato o disabilitato. Se desiderate cambiare lo stato del Controllo della Privacy, deselezionare o selezionare la casella corrispondente.

Importante

Per evitare il furto e proteggere la vostra privacy, mantenere il **Controllo della Privacy** attivo.

Il Controllo della Privacy protegge il vostro computer utilizzando questi importanti controlli di protezione:

- Controllo Identità - protegge i vostri dati riservati filtrando tutto il traffico web (HTTP), mail (SMTP), e chat in uscita secondo le regole da voi create nella sezione Identità.
- Controllo di Registro - chiede il vostro permesso ogni volta che un programma cerca di modificare una chiave di registro per essere eseguita all'avvio di Windows.
- Controllo dei Cookie - chiederà il vostro consenso ogni volta che un sito web tenterà di impostare un cookie.
- Controllo degli Script - chiederà il vostro consenso ogni volta che un sito web tenterà di attivare uno script o un altro contenuto attivo.

Nel lato inferiore della sezione è possibile vedere le **Statistiche Controllo della Privacy**.

20.1.1. Configurazione del Livello di Protezione

Potete scegliere il livello di protezione che meglio si adatta alle vostre necessità di sicurezza. Trascinate il pulsante sulla barra per impostare il livello di protezione appropriato.

Ci sono 3 livelli di protezione:

Livello di protezione	Descrizione
Permissiva	Tutti i controlli di protezione sono disabilitati.
Default	Solo il **Controllo di Identità** è abilitato.
Aggressiva	**Controllo Identità**, **Controllo Registro**, **Controllo Cookie** e **Controllo Script** sono abilitati.

E' possibile personalizzare il livello di protezione cliccando **Livello Personalizzato**. Nella finestra che apparirà, selezionare i controlli di protezione che volete abilitare e cliccare su **OK**.

Cliccando su **Predefinito** verranno applicate le impostazioni di default.

20.2. Controllo Identità

Tenere sicuri i dati riservati è una questione importante che ci preoccupa tutti. I furto di dati ha tenuto il passo con lo siluppo delle comunicazioni via Internet e fa

uso di nuovi metodi per ingannare le persone inducendole a dare via informazioni private.

Che sia la vostra e-mail o il numero della vostra carta di credito, quando finiscono nelle mani sbagliate tali informazioni possono recarvi danno: potete trovarvi affogati nei messaggi di spam o potreste essere sorpresi nell'accedere ad un conto svuotato.

Il Controllo Identità vi protegge dal furto di dati sensibili quando siete online. Basandosi sulle regole create da voi, il Controllo Identità esegue la scansione del traffico web, mail ed instant messaging in uscita dal vostro computer, cercando specifiche sequenze di caratteri (ad esempio, la vostra carta d'identità). Se c'è una coincidenza, la pagina web, la mail o il messaggio instantaneo vengono bloccati.

Potete creare regole per proteggere ogni informazione che considerate personale o confidenziale, dal vostro numero di telefono o il vostro inidrizzo mail alle informazioni sul vostro conto in banca. Viene fornito un supporto Multi-utente, in modo che gli utenti che accedano ad altri account di Windows possano configurare ed usare le proprie regole di protezione dell'identità. Se il proprio account Windows è un account amministratore, le regole create possono essere configurate per essere applicate anche quando altri utenti del computer accedono ai rispettivi account utente Windows.

Perché usare il Controllo Identità?

- Il controllo identità è molto efficace nel bloccare lo spyware keylogger. Questo tipo di applicazione maligna registra le vostre battute sulla tastiera e le invia tramite Internet ad un hacker. L'hacker può trovare informazioni sensibili nei dati rubati, come i numeri e password di un conto corrente, ed usarle per ottenere benefici personali.

  Supponendo che tale applicazione riesca ad evitare la rilevazione antivirus, non potrà inviare i dati rubati via e-mail, web o chat se avete creato regole appropriate per la protezione dell'identità.

- Il Controllo identità vi può proteggere dai tentativi di phishing (tentativi di rubare informazioni personali). I tentativi più comuni di phishing fanno uso di e-mail ingannevoli per convincervi ad inviare informazioni personali ad una falsa pagina web.

  Ad esempio, potreste ricevere una mail che si proclama venire dalla vostra banca e vi richiede di aggiornare urgentemente le informazioni sul vostro conto. La mail vi fornisce un link alla pagina web dove dovreste inserire vostre informazioni personali. Anche se sembrano legittime, le mail e le pagine web alle quali vi conduce il falso link sono fasulle. Se cliccate sul link nella mail ed inviate le vostre informazioni personali alla falsa pagina web, svelerete queste informazioni alle persone che hanno organizzato il tentativo di phishing.

  Se ci sono le appropriate regole di protezione dell'identità, non potrete inviare informazioni personali (come il numero della vostra carta di credito) ad una pagina

web, a meno che non abbiate esplicitamente definito un'eccezione per questa pagina.

Per configurare il Controllo Identità, fare clic su **Controllo della Privacy>Identità** in Modalità avanzata.

Controllo Identità

Se volete usare il Controllo Identità, seguire questi passi:

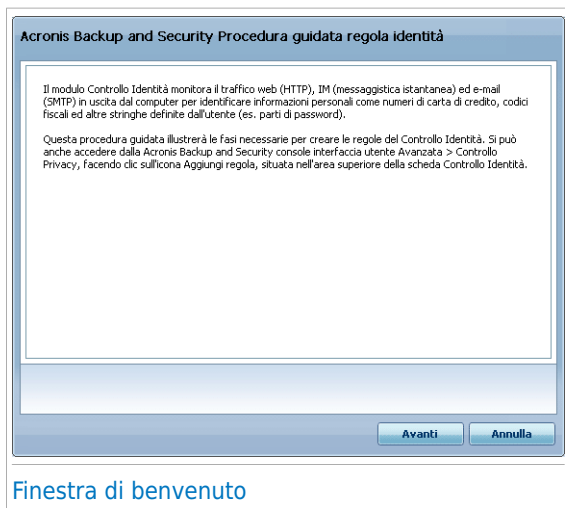
1. Selezionare la casella di controllo **Abilita controllo Identità**.
2. Creare regole per proteggere i vostri dati sensibili. Per ulteriori informazioni, vi preghiamo di riferirvi a «*Creazione delle Regole d'Identità*» (p. 201).
3. Se necessario, definire esclusioni specifiche alle regole create. Per ulteriori informazioni, vi preghiamo di riferirvi a «*Definizione Esclusioni*» (p. 204).
4. Se si è un amministratore del computer, è possibile escludere se stessi dalle regole di identità create da altri amministratori.

   Per ulteriori informazioni, fare riferimento a «*Regole definite da altri amministratori*» (p. 206).

20.2.1. Creazione delle Regole d'Identità

Per creare una regola di protezione dell'identità, fare clic sul pulsante **Aggiungi** e seguire procedura guidata di configurazione.

Passo 1/4 - Finestra di Benvenuto

Finestra di benvenuto

Selezionare **Avanti**.

Passo 2/4 - Impostazione Tipo di Regola e Dati

Impostare il Tipo di Regola e i Dati

Dovete impostare i parametri seguenti:

- **Nome Regola** - inserire il nome della regola nel campo di modifica.
- **Tipo di Regola** - scegliere il tipo di regola (indirizzo, nome, carta di credito, PIN, SSN etc).
- **Dati Regola** - inserire i dati da proteggere nel campo di modifica. Ad esempio, se si vuole proteggere la carta di credito, inserire tutto o parte del numero in questo campo.

Nota
Se inserite meno di tre caratteri, vi verrà chiesto di validare i dati. Vi consigliamo di inserire al meno tre caratteri per evitare il blocco erroneo di messaggi e pagine web.

Tutti i dati che inserite sono criptati. Per una sicurezza maggiore, non inserire tutti i dati che volete proteggere.

Selezionare **Avanti**.

Passo 3/4 - Selezionare i Tipi di Traffico e gli Utenti

Selezionare i Tipi di Traffico e gli Utenti

Selezionare il traffico che si desidera esaminare con Acronis Backup and Security 2010. Sono disponibili le seguenti opzioni:

- **Scansione web (traffico HTTP)** - scansiona il traffico HTTP (web) e blocca i dati in uscita corrispondenti ai dati della regola.
- **Scansione e-mail (traffico SMTP)** - esamina il traffico SMTP (mail) e blocca le mail in uscita contenenti i dati della regola.
- **Scansione IM (Instant Messaging)** - scansiona il traffico Instant Messaging e blocca i messaggi in uscita contenenti i dati della regola.

Potete scegliere di applicare la regola solo se i dati della regola corrispondono completamente oppure se le maiuscole/minuscole corrispondono.

Specificare gli utenti a cui si applica la regola.

- **Solo per me (utente attuale)** - la regola si applica solo all'account utente attuale.
- **Account utente limitati** - la regola si applica all'utente attuale e a tutti gli account di Windows limitati.
- **Tutti gli utenti** - la regola si applica a tutti gli account di Windows.

Selezionare **Avanti**.

Passo 4/4 – Descrizione Regola

Definizione Regola

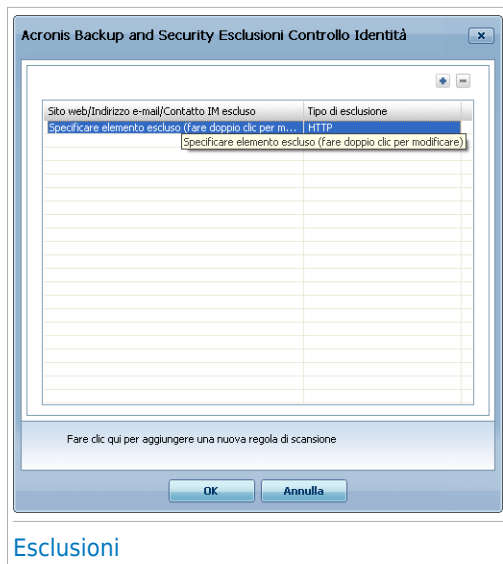
Inserire una breve descrizione della regola nel campo di editing. Siccome i dati bloccati (serie di caratteri) non vengono mostrati in plain text quando si accede alla regola, la descrizione dovrebbe aiutarvi ad identificarla facilmente.

Selezionare **Termina**. La regola apparirà nella tabella.

20.2.2. Definizione Esclusioni

Ci sono dei casi in cui dovrete definire eccezioni a specifiche regole d'identità. Consideriamo il caso in cui voi create una regola che impedisca l'invio attraverso HTTP (web) del numero della vostra carta di credito. Ogni volta che il numero della vostra carta di credito verrà inviato ad un sito web dal vostro account, la rispettiva pagina verrà bloccata. Se volete, per esempio, comprare delle scarpe in un negozio on line (che sapete che è sicuro), dovrete specificare un'eccezione alla rispettiva regola.

Per aprire la finestra dove si possono gestire le eccezioni, fare clic su **Esclusioni**.

Esclusioni

Per aggiungere un'eccezione, seguire i seguenti passi:

1. Selezionare **Aggiungi** per aggiungere una nuova regola alla tabella.
2. Fare doppio clic su **Specifica elementi esclusi** e fornire gli indirizzi web, mail o chat che si desidera vengano aggiunti come eccezione.
3. Fare clic due volte su **Tipo traffico** e scegliere dal menu l'opzione corrispondente al tipo d'indirizzo fornito in precedenza.
   - Se avete scelto un indirizzo web, selezionare **HTTP**.
   - Se avete specificato un indirizzo mail, selezionare **E-mail (SMTP)**.
   - Se avete specificato un contatto chat, selezionare **Chat**.

Per rimuovere un'eccezione dall'elenco, selezionarla e fare clic sul pulsante **Rimuovi**.

Selezionare **Applica** per salvare le modifiche.

20.2.3. Amministrazione delle regole

Potete visualizzare l'elenco delle regole create finora nella tabella.

Per eliminare una regola, selezionarla e fare clic sul pulsante **Elimina**.

Per modificare una regola, selezionarla e fare clic sul pulsante **Modifica** oppure fare doppio clic su di essa. Apparirà una nuova finestra.

Modifica Regola

Qui potete modificare il nome, la definizione e i parametri della regola (tipo, dati e traffico). Cliccate su **OK** per salvare le modifiche.

20.2.4. Regole definite da altri amministratori

Se non si è l'unico utente con diritti di amministratore sul sistema, gli altri amministratori possono creare regole di identità a proprio piacimento. Nel caso si desideri che le regole create da altri utenti non si applichino quando si è effettuato l'accesso, Acronis Backup and Security 2010 permette di escludere se stessi da qualsiasi regola che non si sia creata.

È possibile vedere un elenco di regole create da altri amministratori nella tabella sotto la voce **Regole di controllo Identità**. Per ogni regola viene elencato il nome e l'utente che l'ha creata.

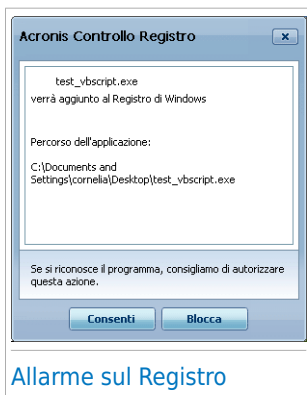
Per escludersi da una regola, selezionarla nella tabella e fare clic sul pulsante **Elimina**.

20.3. Controllo dei Registri

Una componente molto importante del sistema operativo di Windows si chiama **Registro**. E’ dove Windows tiene le informazioni relative alle proprio configurazioni, ai programmi installati, all’utente e così via.

Il **Registro** è inoltre utilizzato per definire quali Programmi devono essere eseguiti automaticamente all'avvio di Windows. Spesso i virus lo utilizzano per essere eseguiti automaticamente quando l'utente riavvia il proprio computer.

Il **Controllo dei Registri** sorveglia il Registro di Windows – azione utile per rilevare i Trojan (Cavalli di Troia). Vi avviserà ogni volta che un programma tenterà di modificare una entrata del registro per poter essere eseguito all'avvio di Windows.

Allarme sul Registro

Potete vedere il programma che sta tentando di modificare il Registro di Windows.

Se non riconoscete il programma e vi sembra sospetto, cliccare su **Bloccare** per impedirgli di modificare il Registro di Windows. Altrimenti, cliccare su **Consentire** per permettere la modifica.

In base alla vostra risposta, viene creata una regola e viene elencata nella tabella delle regole. La stessa azione viene applicata ogni volta che questo programma tenta di modificare una chiave di registro.

Nota

Acronis Backup and Security 2010 vi avviserà, di norma, quando installerete nuovi programmi che necessitano di esecuzione immediata dopo il successivo avvio del vostro computer. Nella maggior parte dei casi questi programmi sono leciti e ci si può fidare.

Per configurare il Controllo di Registro, andare a **Controllo della Privacy>Registro** in Modalità Avanzata.

Controllo dei Registri

Potete visualizzare l'elenco delle regole create finora nella tabella.

Per eliminare una regola, selezionarla e fare clic sul pulsante **Elimina**.

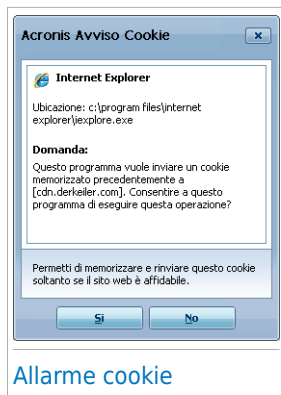
20.4. Controllo dei Cookie

I cookie sono molti frequenti su Internet. Si tratta di piccoli file immagazzinati sul vostro computer. I siti web creano questi cookie per tenere traccia di specifiche informazioni che vi riguardano.

Generalmente i Cookie vengono creati per rendere facilitare le cose. Ad esempio possono aiutare i siti web a ricordare il vostro nome e le vostre preferenze, così da non doverli inserire ad ogni visita.

I cookie però possono anche essere utilizzati per compromettere la vostra riservatezza, tenendo traccia delle vostre abitudini di navigazione.

E’ qui che il **Controllo dei Cookie** vi sarà di aiuto. Quando è attivato, il **Controllo dei Cookie** chiederà il vostro permesso ogni volta che un sito web tenta di impostare un cookie:

Allarme cookie

E' possibile visualizzare il nome dell'applicazione che sta tentando di inviare il file cookie.

Fare clic su **Sì** o **No** e una regola verrà creata, applicata ed elencata nella tabella delle regole.

Ciò aiuterà a scegliere i siti web di cui ci si fida e quelli di cui non ci si fida.

Nota

A causa del notevole numero di cookie utilizzati oggi giorno su Internet, il **Controllo dei Cookie** può risultare inizialmente abbastanza noioso. All'inizio porrà molte domande riguardo ai siti che tentano di piazzare i cookie sul vostro computer. Non appena si aggiungeranno i vostri siti abituali all'elenco delle regole, la navigazione diventerà semplice come prima.

Per configurare il Controllo dei Cookie, fare clic su **Controllo della Privacy>Cookie** in Modalità Avanzata.

Controllo dei Cookie

Potete visualizzare l'elenco delle regole create finora nella tabella.

Per eliminare una regola, selezionarla e fare clic sul pulsante **Elimina**. Per modificare i parametri della regola, fare clic sul pulsante **Modifica** o fare doppio clic su di essa. Eseguire i cambiamenti desiderati nella finestra di configurazione.

Per aggiungere manualmente una regola, fare clic sul pulsante **Aggiungi** e configurare i parametri della regola nella finestra di configurazione.

20.4.1. Finestra di Configurazione

Quando modificate o aggiungete manualmente una regola apparirà la finestra di configurazione.

Seleziona Indirizzo, Azione e Direzione

Potete impostare i parametri:

- **Dominio** - digitare il dominio sul quale applicare la regola.
- **Azione** - selezionare l'azione della regola.

Azione	Descrizione
Permetti	I cookie da quel dominio verranno eseguiti.
Impedisci	I cookie da quel dominio non verranno eseguiti.

- **Direzione** - seleziona la direzione del traffico.

Direzione	Descrizione
In Uscita	La regola verrà applicata solo per i cookie che vengono rispediti al sito connesso.
In Entrata	La regola verrà applicata solo per i cookie che vengono ricevuti dal sito connesso.
Entrambe	La regola sarà applicata in entrambe le direzioni.

Nota

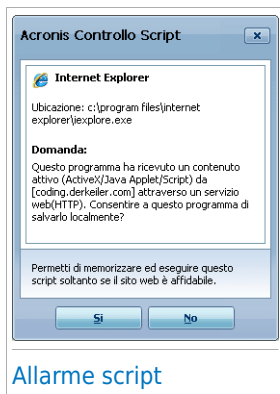
Si possono accettare i cookie, ma non conviene mai rispedirli, cioè impostando l'azioneo **Divieto** e la direzione **Uscente**.

Selezionare **Termina**.

20.5. Controllo script

Gli Scripts e altri codici come ActiveX controls e Java applets, che sono utilizzati per creare pagine interattive, possono essere programmati per avere effetti dannosi. Per esempio gli elementi ActiveX , possono ottenere l' accesso ai dati del vostro computer, cancellare informazioni, catturare passwords e intercettare messaggi mentre siete online. Dovreste accettare contenuti attivi esclusivamente da siti che si conoscono come affidabili.

Acronis Backup and Security 2010 vi consente di scegliere se eseguire questi elementi o bloccare la loro esecuzione.

Con il **Controllo degli Script** sarete coinvolti nel decidere di quali siti web vi fidate e di quali non vi fidate. Acronis Backup and Security 2010 chiederà il vostro permesso ogni volta che un sito web tenta di attivare uno script o altri contenuti attivi:

Allarme script

E' possibile visualizzare il nome della risorsa.

Fare clic su **Sì** o **No** e una regola verrà creata, applicata ed elencata nella tabella delle regole.

Per configurare il Controllo degli Script, fare clic su **Controllo della Privacy>Script** in Modalità Avanzata.

Controllo script

Potete visualizzare l'elenco delle regole create finora nella tabella.

Per eliminare una regola, selezionarla e fare clic sul pulsante **Elimina**. Per modificare i parametri della regola, fare clic sul pulsante **Modifica** o fare doppio clic su di essa. Eseguire i cambiamenti desiderati nella finestra di configurazione.

Per creare manualmente una regola, fare clic sul pulsante **Aggiungi** e configurare i parametri della regola nella finestra di configurazione.

20.5.1. Finestra di Configurazione

Quando modificate o aggiungete manualmente una regola apparirà la finestra di configurazione.

Selezionare Indirizzo ed Azione

Potete impostare i parametri:

- **Dominio** - digitare il dominio sul quale applicare la regola.
- **Azione** - selezionare l'azione della regola.

Azione	Descrizione
Permetti	Gli script da quel dominio verranno eseguiti.
Impedisci	Gli script da quel dominio non verranno eseguiti.

Selezionare **Termina**.

21. Firewall

Il Firewall protegge il vostro computer dai tentativi di connessione non autorizzati sia in entrata che in uscita. E' come una guardia al vostro cancello – manterrà sotto controllo la vostra connessione Internet e terrà traccia di coloro ai quali si concede di accedere ad Internet e di coloro ai quali non è permesso.

Nota

Un firewall è essenziale se si dispone di una banda larga o di una connessione DSL.

In Modalità Invisibile, il vostro computer risulta "nascosto" a software maligni e hacker. Il modulo Firewall è in grado di rilevare automaticamente e proteggere il computer contro i portscan (flusso di pacchetti spediti a una macchina per trovare "punti di accesso", spesso in preparazione di un attacco).

21.1. Impostazioni

Per configurare la protezione firewall, fare clic su **Firewall>Impostazioni** in Modalità Avanzata.

Impostazioni del Firewall

Potete vedere se il firewall Acronis Backup and Security 2010 è abilitato o disabilitato. Se desiderate modificare lo stato del firewall, deselezionare o selezionare la casella corrispondente.

Importante

Per essere protetti contro gli attacchi via Internet, mantenere il **Firewall** abilitato.

Ci sono due categorie di informazioni:

- **Configurazione di rete Abbreviata.** Potete vedere il nome del vostro computer, il suo indirizzo IP ed il gateway di default. Se avete più di un adattatore di rete (significa che siete connessi a più di una rete), vedrete l'indirizzo IP ed il gateway configurati per ogni adattatore.
- **Statistiche.** Potete vedere diverse statistiche riguardanti le attività del firewall:
  - numero di byte inviati.
  - numero di byte ricevuti.
  - numero di scansioni di porte rilevate e bloccate da Acronis Backup and Security 2010. Le scansioni delle porte vengono usate frequentemente dagli hackers per trovare porte aperte sul vostro computer con l'intenzione di sfruttarle.
  - numero di pacchetti persi.
  - numero di porte aperte.
  - numero di connessioni in entrata attive.
  - numero di connessioni in uscita attive.

Per vedere le connessioni attive e le porte aperte, fare clic sulla scheda Attività.

Nel lato inferiore della sezione potete vedere le statistiche Acronis Backup and Security 2010 a proposito del traffico in arrivo e in uscita. Il grafico mostra il volume del traffico internet degli ultimi due minuti.

Nota

Il grafico appare anche se il **Firewall** è disabilitato.

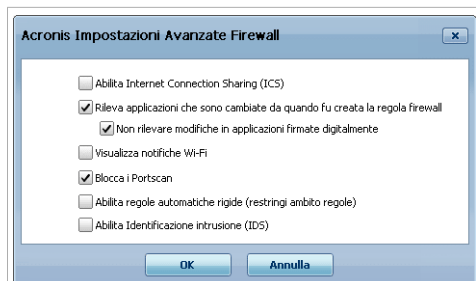
21.1.1. Impostare l'Azione di Default

Di default, Acronis Backup and Security 2010 permette automaticamente a tutti i programmi conosciuti presenti nella sua white list di accedere ai servizi di rete e ad Internet. Per tutti gli altri programmi, Acronis Backup and Security 2010 vi chiede tramite una finestra di allarme di specificare l'azione da intraprendere. L'azione da voi specificata viene intrapresa ogni volta che la rispettiva applicazione richiede l'accesso alla rete / Internet.

Potete trascinare il pulsante scorrevole lungo la barra per impostare l'azione da intraprendere di default sulle applicazioni che richiedono accesso alla rete/Internet. Sono disponibili le seguenti azioni di default:

Azione di default	Descrizione
Consenti tutto	Applica le regole correnti e permette tutti i tentativi di traffico che non corrispondono con le regole correnti senza chiedere il consenso. Questa policy è vivamente sconsigliata però potrebbe essere utile per amministratori di rete e giocatori (gamers).
Consenti Programmi Conosciuti	Applica le regole correnti e consente tutti i tentativi di connessione in uscita dai programmi conosciuti come legittimi (White List) da Acronis Backup and Security 2010 senza chiedere il consenso. Per il resto dei tentativi di connessione, Acronis Backup and Security 2010 vi chiederà il permesso. I programmi inclusi nella White List sono le applicazioni più comunemente utilizzate al mondo. Includono i browser più conosciuti, riproduttori audio & video, programmi di chat e condivisione file, così come applicazioni client server e di sistema operativo. Per vedere la whitelist completa, fare clic su **Visualizza Whitelist**.
Report	Applica le regole correnti e chiede su tutti i tentativi di traffico che non corrispondono ad una qualunque delle regole correnti di consenso.
Rifiuta tutto	Applica le regole correnti e blocca tutti i tentativi di traffico che non corrispondono ad una qualunque delle regole correnti.

21.1.2. Configurazione delle Impostazioni Avanzate del Firewall

È possibile fare clic su **Impostazioni Avanzate** per configurare le impostazioni avanzate del firewall.

Impostazioni Avanzate del Firewall

Sono disponibili le seguenti opzioni:

- **Abilita il supporto Condivisione Connessione Internet(ICS)** - abilita il supporto per la Condivisione Connessione Internet (ICS).

  Nota
  Questa opzione non abilita automaticamente ICS sul vostro sistema, ma consente solo questo tipo di connessione nel caso voi la abilitiate dal vostro sistema operativo.

  La Condivisione della Connessione Internet (ICS) permette ai membri delle reti locali di collegarsi ad Internet attraverso il vostro computer. Ciò è utile quando usufruite di una connessione Internet speciale/particolare (es. connessione wireless) e volete condividerla con altri membri della vostra rete.

  Condividere la vostra connessione Internet con i membri delle reti locali porta ad un livello di consumo risorse più alto e può comportare un certo rischio. Taglia anche alcune delle vostre porte (quelle aperte dai membri che stanno utilizzando la vostra connessione Internet).

- **Rileva applicazioni che cambiano da quando la regola di firewall è stata creata** - verifica ogni applicazione che tenta di connettersi a Internet per vedere se è stata cambiata da quando la regola che ne controlla l'accesso è stata aggiunta. Se l'applicazione è stata cambiata, verrà visualizzato un avviso per consentire o bloccare l'accesso dell'applicazione a Internet.

  Normalmente, le applicazioni vengono modificate dagli aggiornamenti. Ma c'è il rischio che vengano modificate da applicazioni malware, con il proposito di infettare il vostro computer ed altri computer in rete.

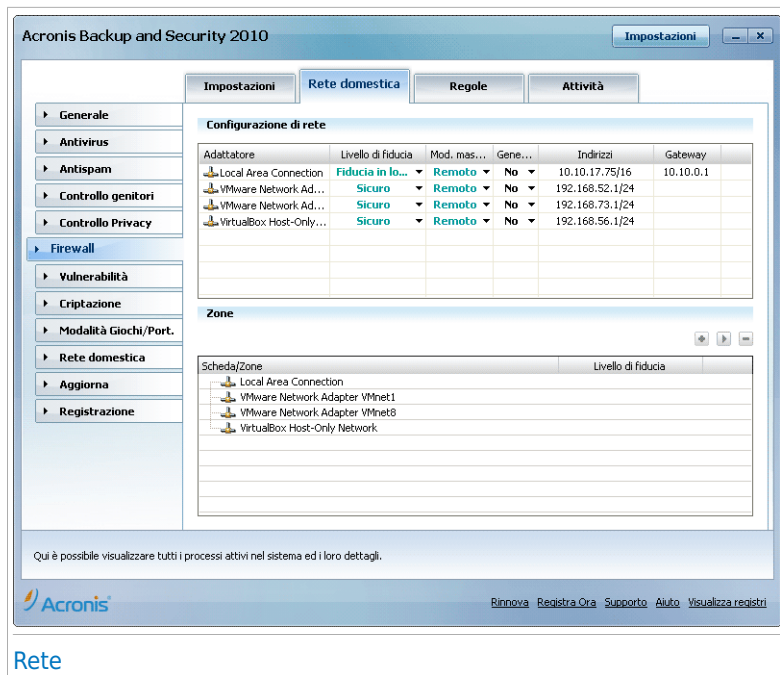
  Nota
  Vi consigliamo di mantenere attiva questa opzione e di consentire l'accesso solo alle applicazioni che vi aspettate vengano modificate dopo che la regola di controllo del loro accesso è stata creata.

Le applicazioni segnalate si suppone che siano di fiducia e che abbiano un più alto grado di sicurezza. È possibile selezionare **Ignora le modifiche in applicazioni firmate digitalmente** per consentire alle applicazioni firmate cambiate di connettersi ad Internet senza ricevere un avviso su questo evento.

- **Visualizza notifiche wireless** - se si è connessi ad una rete wireless, mostra delle finestre informative relative a specifiche eventualità sulla rete (ad esempio, quando un nuovo computer è entrato in rete).
- **Bloccare le scansioni delle porte** - rileva e blocca i tentativi di scoprire quali porte sono aperte.

  Le scansioni delle porte vengono comunemente usate dai hacker per scoprire quali porte sono aperte sul vostro computer. Potrebbero quindi introdursi nel vostro computer se trovassero una porta meno sicura o vulnerabile.
- **Abilita regole automatiche rigide** - crea regole rigide utilizzando la finestra di allarme del firewall. Con questa opzione selezionata, Acronis Backup and Security 2010 vi chiederà di attuare e creerà regole per ogni processo che apra l'applicazione che richieda l'accesso alla rete o ad Internet.
- **Abilita sistema di rilevamento d'intrusione (IDS)** - attiva il monitoraggio euristico delle applicazioni che tentano l'accesso ai servizi di rete o ad Internet.

21.2. Rete

Per configurare le impostazioni del firewall, fare clic su **Firewall>Rete** in Modalità Avanzata.

Rete

Le colonne della tabella **Configurazione di Rete** fornisce informazioni dettagliate sulla rete alla quale siete connessi:

- **Adattatore** - l'adattatore di rete che usa il vostro computer per connettersi alla rete o ad Internet.
- **Livello di attendibilità** - il livello di fiducia assegnato alla scheda di rete. A seconda della configurazione del adattatore di rete, Acronis Backup and Security 2010 potrebbe assegnare automaticamente all'adattatore un livello di fiducia o richiedervi ulteriori informazioni.
- **Modalità invisibile** - se si può essere rilevati da altri computer o meno.
- **Profilo generico** - se delle regole generiche vengono applicate a questa connessione o meno.
- **Indirizzi** - gli indirizzi IP configurati sull'adattatore.
- **Gateway** - l'indirizzo IP che utilizza il vostro computer per connettersi ad Internet.

21.2.1. Modifica del Livello di Fiducia

Acronis Backup and Security 2010 assegna ad ogni adattatore di rete un livello di fiducia. Il livello di fiducia assegnato all'adattatore indica quanto è attendibile la corrispondente rete.

Basandosi sul livello di fiducia, delle regole specifiche vengono create per l'adattatore riguardo a come il sistema ed i processi di Acronis Backup and Security 2010 accedono alla rete e ad Internet.

È possibile vedere il livello di fiducia configurato per ogni scheda nella tabella **Configurazione di Rete**, nella colonna **Livello di attendibilità**. Per modificare il livello di fiducia, fare clic sulla freccia della colonna **Livello di attendibilità** e selezionare il livello desiderato.

Livello di fiducia	Descrizione
Piena fiducia	Disabilita il firewall per il relativo adattatore.
Locale di fiducia	Consente tutto il traffico tra il vostro computer ed i computer nella rete locale.
Sicuro	Consente la condivisione di risorse con i computer nella rete locale. Questo livello viene automaticamente impostato per le reti locali (domestica o ufficio).
Non sicuro	Blocca la connessione dei computer dalla rete o da Internet al vostro computer. Questo livello viene automaticamente impostato per le reti pubbliche (se avete ricevuto un indirizzo IP da un Provider di servizi Internet)
Locale bloccato	Blocca tutto il traffico tra il vostro computer ed i computer nella rete locale mentre siete connessi ad Internet. Questo livello di fiducia viene automaticamente impostato per le reti wireless non sicure (aperte).
Bloccato	Blocca completamente la rete ed il traffico Internet attraverso il relativo adattatore.

21.2.2. Configurare la Modalità Invisibile

La Modalità Invisibile nasconde il vostro computer dal software maligno e dagli hacker in rete o in Internet. Per configurare la Modalità Invisibile, cliccare sulla freccia ▾ nella colonna **Cautela** e selezionare l'opzione desiderata.

Opzione Invisibile	Descrizione
Attivare.	La Modalità Invisibile è attiva. Il vostro computer è invisibile sia dalla rete locale che da Internet.

Opzione Invisibile	Descrizione
Disattivare	La Modalità Invisibile è disattivata Tutti possono pingare e rilevare il vostro computer dalla rete locale o da Internet.
Remoto	Il vostro computer non può essere rilevato da Internet. Gli utenti locali possono pingare e rilevare il vostro computer.

21.2.3. Configurare le Impostazioni Generali

Se l'indirizzo IP di un adattatore di rete viene modificato, Acronis Backup and Security 2010 modificherà il livello di ficucia di conseguenza. Se desiderate mantenere lo stesso livello di fiducia, cliccare sulla freccia nella colonna **Generico** e selezionare **Si**.

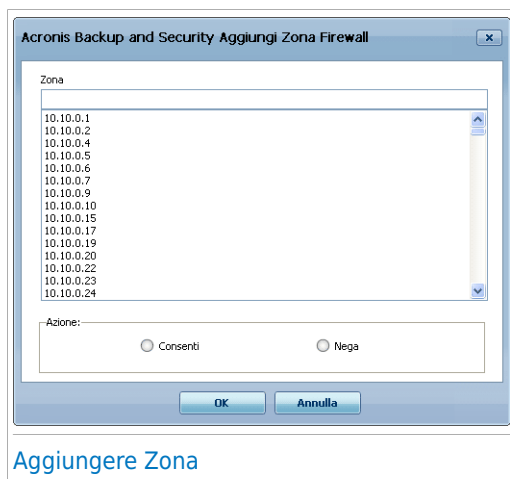
21.2.4. Zone di rete

Potete aggiungere dei computer consentiti o bloccati per un adattatore specifico.

Una zona di fiducia è un computer del quale vi fidate pienamente. Tutto il traffico tra il computer ed un computer affidabile è consentito. Per condividere delle risorse con un computer specifico in una rete wireless non sicura, aggiungerli come computer consentiti.

Una zona bloccata è un computer che non volete assolutamente che comunichi con il vostro computer.

La tabella **Zone** mostra le zone di rete correnti per adattatore.

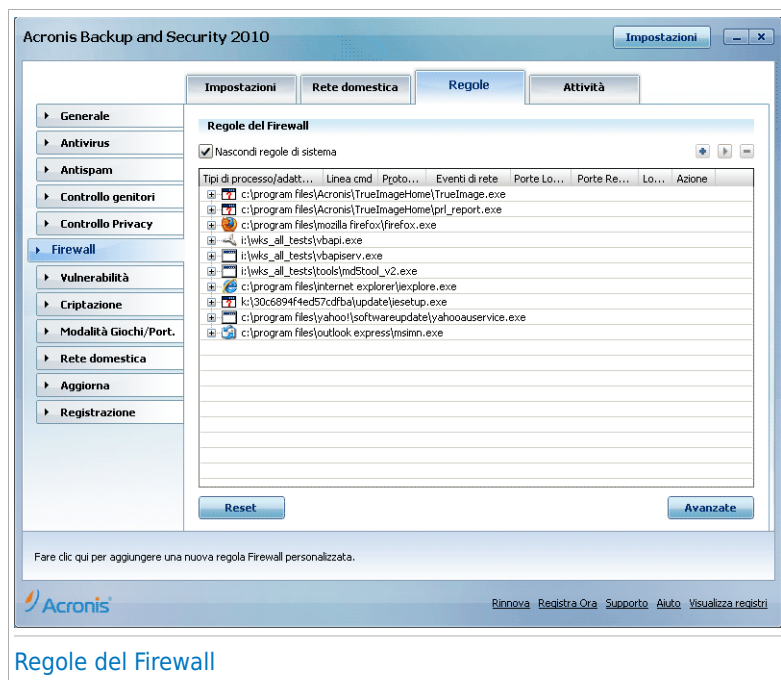
Per aggiungere una zona, fare clic sul pulsante **Aggiungi**.

Aggiungere Zona

Procedere come segue:

1. Selezionare l'indirizzo IP del computer che volete aggiungere.
2. Selezionare l’azione:
   - **Consentire** - per consentire tutto il traffico tra il vostro computer ed il computer selezionato.
   - **Rifiutare** - per bloccare tutto il traffico tra il vostro computer ed il computer selezionato.
3. Selezionare **OK**.

21.3. Regole

Per gestire le regole del firewall che controllano l'accesso delle applicazioni alle risorse di rete o ad Internet, andare su **Firewall>Regole** in Modalità Avanzata.

Regole del Firewall

Potete vedere le applicazioni (processi) per le quali le regole del firewall sono state create. Deselezionare la casella **Nascondere le regole di sistema** se desiderate vedere anche le regole relative al sistema o ai processi di Acronis Backup and Security 2010.

Per vedere le regole create per un'applicazione specifica, cliccare sulla casella + accanto alla relativa applicazione. Potete sapere le informazioni dettagliate su ogni regola, come indicato nelle colonne della tabella:

- **Tipologie di processo/adattatore** - le tipologie di processo e adattatore di rete sui quali vengono applicate le regole. Le regole vengono create automaticamente per filtrare l'accesso alla rete o ad Internet attraverso tutti gli adattatori. Potete creare nuove regole manualmente o modificare regole esistenti per filtrare l'accesso alla rete o ad Internet di un'applicazione attraverso un adattatore specifico (ad esempio, un adattatore di rete wireless).
- **Linea di Comando** - il comando utilizzato per iniziare il processo nell'interfaccia della linea di comando di Windows (**cmd**).
- **Protocollo** - il protocollo IP al quale si applica la regola. Potrete visualizzare uno dei seguenti:

Protocollo	Descrizione
Qualsiasi	Include tutti i protocolli IP.
TCP	Transmission Control Protocol – Il Protocollo TCP abilita due host a stabilire una connessione e a scambiarsi pacchetti di dati. TCP garantisce la consegna dei dati e anche le garanzie che i pacchetti saranno consegnati nello stesso ordine in cui sono stati inviati.
UDP	User Datagram Protocol – UDP è un IP progettato per prestazioni hig. I giochi e altre applicazioni video utilizzano spesso UDP.
Un numero	Rappresenta un protocollo IP specifico (diverso da TCP e UDP). Potete trovare l'elenco completo dei numeri di protocolli IP assegnati su www.iana.org/assignments/protocol-numbers.

- **Eventi di Rete** - gli eventi di rete sui quali viene applicata la regola. I seguenti eventi possono essere tenuti in conto:

Evento	Descrizione
Connettere	Scambio preliminare di messaggi standard usati da protocolli orientati alla connessione (come il TCP) per stabilire una connessione. Con protocolli orientati alla connessione, il traffico di dati tra due computer accade solo dopo che la connessione è stabilita.
Traffico	Flusso di dati tra due computer.

Evento	Descrizione
Ascoltare	Stato in cui una applicazione monitorizza la rete in attesa di stabilire una connessione o di ricevere informazioni da un'applicazione pari.

- **Porte Locali** - le porte del vostro computer sulle quali la regola viene applicata.
- **Porte Remote** - le porte di computer remoti sulle quali la regola viene applicata.
- **Locale** - se la regola viene applicata solo sui computer nella rete locale.
- **Azione** - se all'applicazione è permesso o vietato l'accesso alla rete o ad Internet sotto le circostanze specificate.

21.3.1. Aggiungere Regole Automaticamente

Con il **Firewall** abilitato, Acronis Backup and Security 2010 chiederà il vostro consenso ogni volta che viene eseguita una connessione ad Internet:

Allarmi del Firewall

Potete vedere quanto segue: l'applicazione che sta provando ad accedere ad Internet, il percorso per il file dell'applicazione, la destinazione, il protocollo utilizzato e la porta sulla quale l'applicazione sta provando a connettersi.

Cliccare **Consentire** per permettere tutto il traffico (in entrata ed in uscita) generato da questa applicazione dall'host locale verso qualsiasi destinazione, attraverso il rispettivo protocollo IP e su tutte le porte. Se cliccate su **Bloccare**, all'applicazione verrà completamente negato l'accesso ad Internet attraverso il rispettivo protocollo IP.

Basandosi sulla vostra risposta, una regola verrà creata, applicata ed inserita nella tabella. La prossima voltra che l'applicazione cercherà di connettersi, questa regola verrà applicata di default.

Importante

Consentire tentativi di connessioni in ingresso solo da IP o domini dei quali vi fidate.

21.3.2. Eliminazione e ripristino delle regole

Per cancellare una regola, selezionarla e cliccare sul tasto **Rimuovere regola**. Potete selezionare ed eliminare diverse regole alla volta.

Se desiderate cancellare tutte le regole create per un'applicazione specifica, selezionare l'applicazione dall'elenco e cliccare sul tasto **Rimuovere regola**.

Se si desidera caricare la regola predefinita per il livello di attendibilità selezionato, fare clic su **Ripristino regole**.

21.3.3. Creare e modificare delle Regole

Creare nuove regole manualmente e modificare regole esistenti consiste in configurare i parametri della regola nella finestra di configurazione.

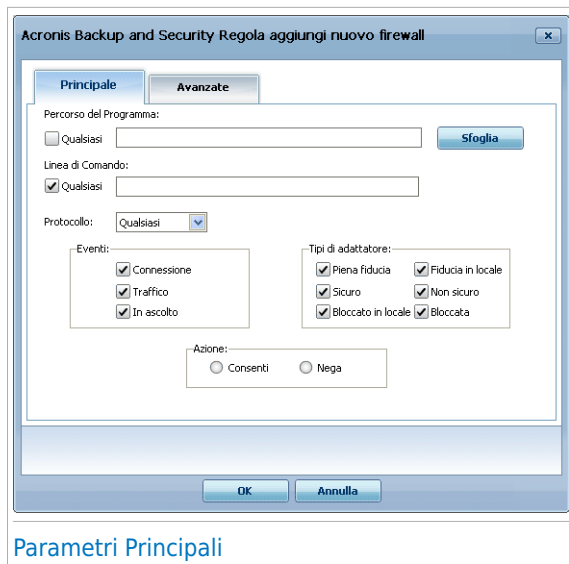
Creare Regole. Per creare una regola manualmente, seguire questi passaggi:

1. Fare clic sul pulsante **Aggiungi regola**. Apparirà la finestra di configurazione.
2. Configurare i parametri principali ed avanzati come necessario.
3. Cliccare su **OK** per aggiungere la nuova regola.

Modificare Regole. Per modificare una regola esistente, seguire i seguenti passaggi:

1. Fare clic sul pulsante **Modifica regola** o fare doppio clic sulla regola. Apparirà la finestra di configurazione.
2. Configurare i parametri principali ed avanzati come necessario.
3. Selezionare **Applica** per salvare le modifiche.

Configurazione dei parametri principali

La scheda **Principali** della finestra di configurazione permette di configurare i parametri principali della regola.

Parametri Principali

E' possibile configurare i seguenti parametri:

- **Percorso del Programma.** Cliccare su **Sfoglia** e selezionare l'applicazione sulla quale viene applicata la regola. Se desiderate che la regola venga applicata su tutte le applicazioni, selezionare **Qualsiasi**.
- **Linea di commando.** Se volete che la regola venga applicata solo quando l'applicazione sia aperta con un comando specifico nell'interfaccia linea di comando di Windows, deselezionare la casella **Qualsiasi** e digitare il comando corrispondente nel campo di modifica.
- **Protocollo.** Selezionare dal menu, il protocollo IP sul quale la regola verrà applicata.
  - Se desiderate che la regola venga applicata su tutti i protocolli, selezionare **Qualsiasi**.
  - Se si desidera che la regola venga applicata a TCP, selezionare **TCP**.
  - Se si desidera che la regola venga applicata a UDP, selezionare **UDP**.
  - Se volete che la regola venga applicata su un protocollo specifico, selezionare **Altro**. Apparirà un campo di modifica. Digitare il numero assegnato al protocollo che volete filtrare nel campo di modifica.

Nota

I numeri dei protocolli IP vengono assegnati dalla Internet Assigned Numbers Authority (IANA). Potete trovare l'elenco completo dei numeri di protocolli IP assegnati su www.iana.org/assignments/protocol-numbers.

- **Eventi.** A seconda del protocollo selezionato, scegliere gli eventi di rete sui quali la regola verrà applicata. I seguenti eventi possono essere tenuti in conto:

Evento	Descrizione
Connettere	Scambio preliminare di messaggi standard usati da protocolli orientati alla connessione (come il TCP) per stabilire una connessione. Con protocolli orientati alla connessione, il traffico di dati tra due computer accade solo dopo che la connessione è stabilita.
Traffico	Flusso di dati tra due computer.
Ascoltare	Stato in cui una applicazione monitorizza la rete in attesa di stabilire una connessione o di ricevere informazioni da un'applicazione pari.

- **Tipi di adattore:** Selezionare i tipi di adattatore a cui si applica la regola.
- **Azione.** Selezionare una delle azioni disponibili:

Azione	Descrizione
Permetti	L'accesso alla rete / Internet dell'applicazione verrà autorizzato quando si verifichino le circostanze specificate.
Impedisci	L'accesso alla rete / Internet dell'applicazione verrà negato le circostanze specificate.

Configurazione dei Parametri Avanzati

La scheda **Avanzati** della finestra di configurazione consente di configurare i parametri avanzati della regola.

Parametri Avanzati

Potete configurare i seguenti parametri avanzati:

- **Direzione.** Selezionare dal menu la direzione del traffico sulla quale verrà applicata la regola.

Direzione	Descrizione
In Uscita	La regola sarà applicata solo per il traffico in uscita.
In Entrata	La regola sarà applicata solo per il traffico in entrata.
Entrambe	La regola sarà applicata in entrambe le direzioni.

- **Versione IP.** Selezionare dal menu la versione IP (IPv4, IPv6 o altre) sulla quale verrà applicata la regola.
- **Indirizzo Locale.** Specificare l'indirizzo IP locale e la porta sui quali verrà applicata la regola come segue:
  - Se avete più di un adattatore di rete, potete deselezionare la casella **Qualsiasi** e digitare un indirizzo IP specifico.
  - Se avete selezionato TCP o UDP come protocollo, potete impostare una porta specifica oppure un range tra 0 e 65535. Se volete la regola applicata per tutte le porte, selezionare **Qualsiasi**.

- **Indirizzo Remoto.** Specificare l'indirizzo IP remoto e la porta sui quali verrà applicata la regola come segue:
  - Per filtrare il traffico tra il vostro computer ed un computer specifico, deselezionare la casella **Qualsiasi** e digitare il suo indirizzo IP.
  - Se avete selezionato TCP o UDP come protocollo, potete impostare una porta specifica oppure un range tra 0 e 65535. Se volete la regola applicata per tutte le porte, selezionare **Qualsiasi**.
- **Applicare questa regola solo su computer connessi direttamente.** Selezionare questa opzione quando volete che la regola venga applicata solo sui tentativi di traffico locale.
- **Controlla la catena dei processi per il processo d'origine.** È possibile modificare questo parametro solo se si seleziona **Regole automatiche rigide** (fare clic sulla scheda Impostazioni e fare clic su **Impostazioni Avanzate**). Il controllo approfondito applicazione significa che Acronis Backup and Security 2010 domanda l'azione da intraprendere quando un'applicazione richiede l'accesso ad Internet/LAN da un processo parente differente (es: la richiesta di accesso ad Internet da parte di Windows Media Player all'interno di Internet Explorer)

21.3.4. Gestione Avanzata delle Regole

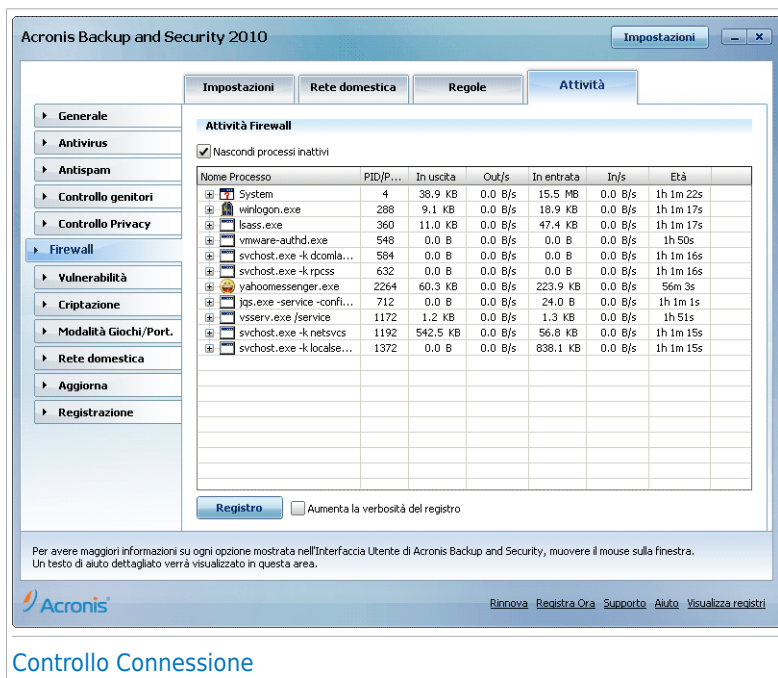
Se avete bisogno del controllo avanzato delle regole del firewall, cliccare su **Avanzate**. Apparirà una nuova finestra.

Gestione Avanzata delle Regole

Potete vedere le regole del firewall, elencate nell'ordine in cui sono state inserite. Le collonne della tabella forniscono informazioni esaustive su ogni regola.

Nota

Quando viene effettuato un tentativo di connessione (sia in entrata che in uscita), Acronis Backup and Security 2010 applica l'azione della prima regola che corrisponde con la connessione. Per questo è molto importante l'ordine in cui le regole vengono selezionate.

Per cancellare una regola, selezionarla e fare clic sul pulsante **Elimina regola**.

Per modificare una regola esistente, selezionarla e fare clic sul pulsante **Modifica regola** oppure fare doppio clic sulla regola.

Potete alzare o abbassare la priorità di una regola. Fare un clck sul bottone **Sposta in alto** per alzare la priorità della regola selezionata di un livello, oppure fare un click sul bottone **Sposta in basso** per abbassare la priorità della regola selezionata, di un livello. Per assegnare ad una regola la massima priorità fare clic sul pulsante **Sposta all'inizio**. Per assegnare ad una regola la minima priorità fare clic sul pulsante **Sposta alla fine**.

Cliccare su **Chiudere** per chiudere la finestra.

21.4. Controllo Connessione

Per monitorare l'attività della rete / Internet corrente (su TCP e UDP) ordinata per applicazioni ed aprire il log del Firewall Acronis Backup and Security 2010, fare clic su **Firewall>Attività** in Modalità Avanzata.

Controllo Connessione

E' possibile visualizzare il traffico totale generato dall'applicazione. Per ogni applicazione, è possibile visualizzare le connessioni e le porte aperte, così come le statistiche riguardanti la velocità del traffico in uscita ed in entrata e la quantità totale di dati inviati / ricevuti.

Se desiderate vedere anche i processi inattivi, deselezionare la casella **Nascondere processi inattivi**.

Il significato delle icone è come segue:

- Indica una connessione in uscita.
- Indica una connessione in entrata.
- Indica una porta aperta sul vostro computer.

La finestra presenta l'attività della rete corrente / Internet in tempo reale. Se le connessioni o le porte fossero chiuse, potreste vedere che le statistiche

corrispondenti sarebbero opache e che, alla fine, scomparirebbero. La stessa cosa accade a tutte le statistiche corrispondenti ad un'applicazione che genera traffico o ha delle porte aperte e che voi chiudete.

Per un elenco esauriente di eventi riguardanti l'utilizzo del modulo Firewall (abilitare/disabilitare il firewall, bloccare il traffico, modificare le impostazioni) o generati dalle attività rilevate da questo modulo (scansione delle porte, blocco di tentativi di connessione o del traffico secondo le regole), visualizzare il file di registro del Firewall Acronis Backup and Security 2010 facendo clic su **Visualizza Registro**.

Se desiderate che il registro contenga più informazioni, selezionare **Incrementare verbosità del registro**.

22. Vulnerabilità

Un passaggio importante nella protezione del vostro computer contro hackers e applicazioni maligne è mantenere aggiornato il sistema operativo e le applicazioni che usate regolarmente. Inoltre, per impedire accessi fisici non autorizzati al vostro computer, dovete configurare password forti (password che non possano essere facilmente indovinate) per ogni account di Windows.

Acronis Backup and Security 2010 controlla regolarmente il vostro sistema alla ricerca di vulnerabilità e vi avverte dei problemi esistenti.

22.1. Stato

Per configurare il controllo automatico delle vulnerabilità o per eseguire un controllo delle vulnerabilità, fare clic su **Vulnerabilità>Stato** in Modalità Avanzata.

Stato Vulnerabilità

La tabella mostra i problemi trovati nell'ultima scansione delle vulnerabilità e il loro stato. Potete vedere l'azione intrapresa per riparare le vulnerabilità, se necessario. Se l'azione **negativa** allora il rispettivo problema non rappresenta una vulnerabilità.

Importante

Per essere avvertiti automaticamente sulle vulnerabilità del sistema o delle applicazioni, mantenere il **Controllo Automatico delle Vulnerabilità** abilitato.

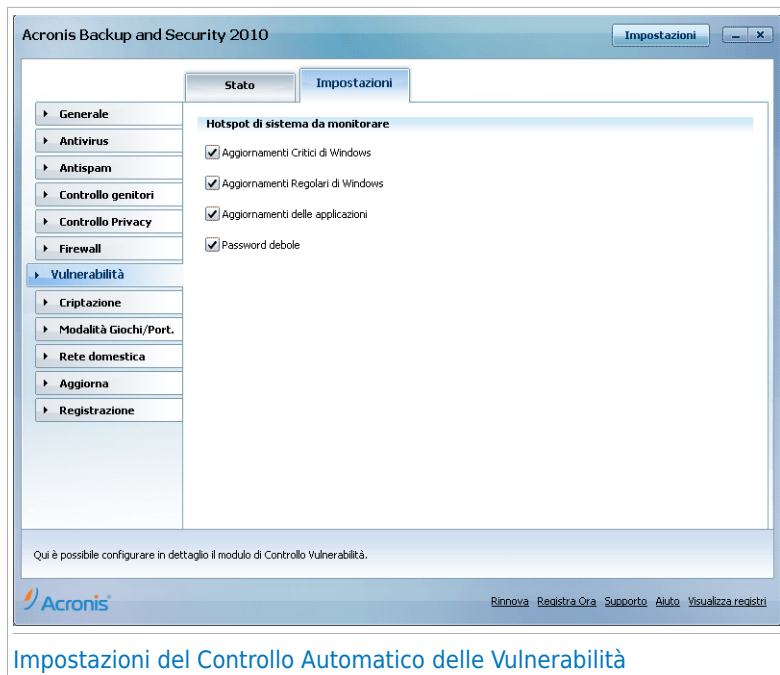
22.1.1. Correggi Vulnerabilità

A seconda del problema, per risolvere una vulnerabilità specifica procedere come segue:

- Se sono disponibili aggiornamenti di Windows, fare clic su **Installa** nella colonna **Azione** per installarli.
- Se un'applicazione non è aggiornata, cliccare sul link fornito **Home Page** per scaricare la versione più recente.
- Se un account utente Windows ha una password debole, fare clic su **Risolvi** per costringere l'utente a modificare la password al prossimo accesso, oppure cambiate voi stessi la password. Per avere una password forte, utilizzare una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, $ o @).

Per controllare le possibili vulnerabilità del vostro computer, clicca su **Controlla adesso** e seguire la procedura guidata. Per ulteriori informazioni fare riferimento a *«Procedura guidata di Controllo delle vulnerabilità»* (p. 58).

22.2. Impostazioni

Per configurare le impostazioni del controllo automatico delle vulnerabilità andare su **Vulnerabilità>Impostazioni** in Modalità Avanzata.

Impostazioni del Controllo Automatico delle Vulnerabilità

Selezionare le caselle corrispondenti alle vulnerabilità del sistema che volete vengano controllate regolarmente.

- **Aggiornamenti Critici di Windows**
- **Aggiornamenti Regolari di Windows**
- **Aggiornamenti applicazioni**
- **Password Deboli**

Nota

Se deselezionate la casella corrispondente ad una vulnerabilità specifica, Acronis Backup and Security 2010 non vi avvertirà più sui relativi problemi.

23. Criptazione

Acronis Backup and Security 2010 offre delle capacità di criptazione per proteggere i vostri documenti confidenziali e le vostre conversazioni attraverso Yahoo Messenger e MSN Messenger.

23.1. Criptazione Chat (IM)

Di default, Acronis Backup and Security 2010 esegue la criptazione di tutte le vostre sessioni chat, purché:

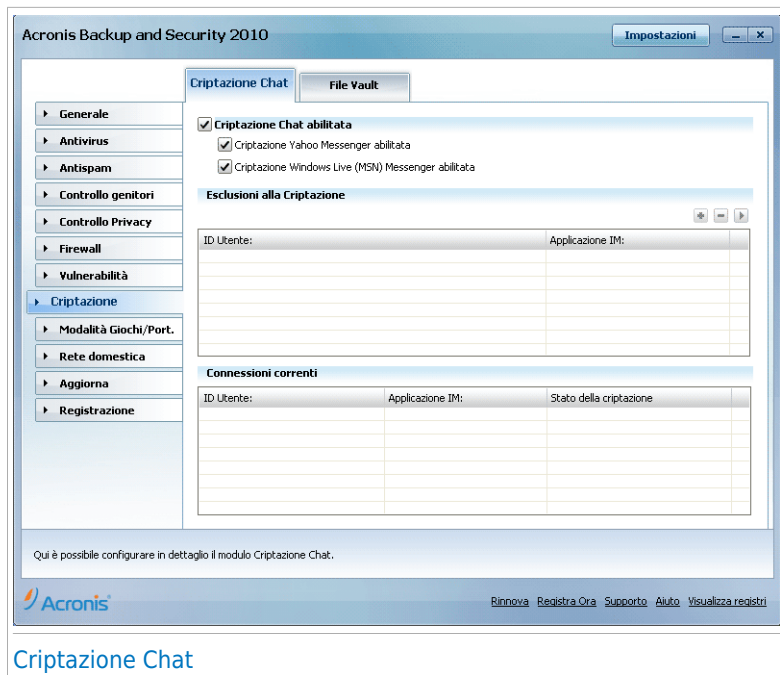
- Il tuo partner di chat abbia un prodotto di Acronis installata che supporti la Criptazione Chat, e la Criptazione Chat sia abilitata per l'applicazione usata per chattare.
- Tu ed il tuo partner di chat usate entrambi Yahoo Messenger o Windows Live (MSN) Messenger.

Importante

Acronis Backup and Security 2010 non eseguirà la criptazione di una conversazione se uno dei partner utilizza un'applicazione chat su web, come Meebo, o se uno dei partner utilizza Yahoo! e l'altro Windows Live (MSN).

Per configurare la criptazione dell'instant messaging, fare clic su **Criptazione>Criptazione IM** in Modalità Avanzata.

Nota

Potete configurare facilmente la criptazione dell'instant messaging utilizzando la barra degli strumenti di Acronis nella finestra di chat. Per ulteriori informazioni fare riferimento a «*Integrazione in Programmi Instant Messenger*» (p. 278).

Criptazione Chat

Di default, la Criptazione Chat è abilitata sia per Yahoo Messenger che per Windows Live (MSN) Messenger. Potete scegliere di disabilitare la Critazione Chat solo per una specifica applicazione di chat o completamente.

Vengono mostrate due tabelle:

- **Esclusioni della Criptazione** - elenca le ID degli utenti ed i relativi programmi di chat per i quali la criptazione è disabilitata. Per rimuovere un contatto dall'elenco, selezionarlo e quindi fare clic sul pulsante ⊟ **Rimuovi**.
- **Connessioni Correnti** - elenca le connessioni in corso di chat (ID utente e programma associato) e se queste sono criptate o meno. Una connessione può non essere criptata per questi motivi:
    - ▶ Avete esplicitamente disabilitato la criptazione per questo contatto.
    - ▶ Il vostro contatto non ha installato un prodotto di Acronis che supporti la Criptazione chat.

23.1.1. Disabilitare la Criptazione per Utenti Specifici

Per disabilitare la criptazione per uno specifico utente, seguire questi passaggi:

1. Fare clic sul pulsante Aggiungi **Aggiungi** per aprire la finestra di configurazione.

Aggiungere Contatti

2. Digitare la ID utente del vostro contatto nel campo corrispondente.
3. Selezionare l'applicazione di instant messaging associata al contatto.
4. Selezionare **OK**.

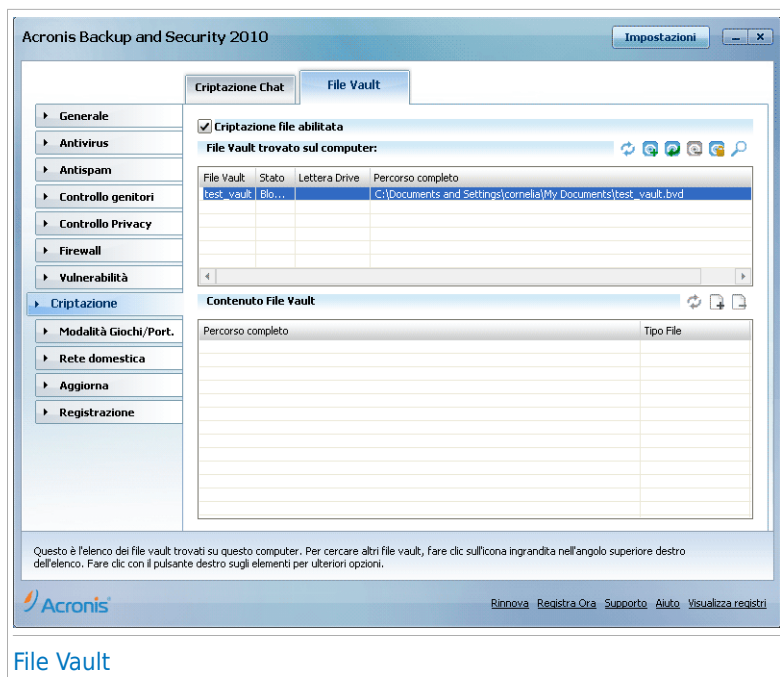
23.2. Criptazione file

La Criptazione File di permette di creare dei drive logici (o vault) criptati e protetti da password sul computer, dove è possibile immagazzinare i documenti confidenziali e sensibili in modo sicuro. L'accesso ai dati immagazzinati in questi vault è consentito solo agli utenti che conoscono la password.

La password vi consente di aprire, immagazzinare dati e chiudere un vault mentre mantenete la sua sicurezza. Mentre un vault è aperto, potete aggiungere dei nuovi file, accedere ai file correnti o modificarli.

Fisicamente, il vault è un file immagazzinato nel disco rigido locale, con l'estensione `.bvd`. Anche se l'accesso ai file fisici che rappresentano i drive protetti è possibile da diversi sistemi operativi (come Linux), le informazioni immagazzinate in essi non possono essere lette perchè criptate.

Per gestire i file vault sul computer, fare clic su **Criptazione>Criptazione File** in Modalità Avanzata.

File Vault

Per disabilitare la Criptazione File, deselezionare la casella **Criptazione File abilitata** e fare clic su **Sì** per confermare. Se disabilitate la Criptazione File, tutti i vault verranno bloccati e non potrete più accedere ai file che li contengono.

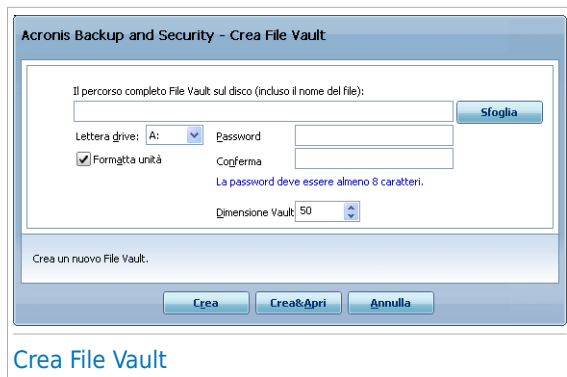
La tabella nella parte superiore mostra i vault sul vostro computer. Potete vedere il nome, lo stato (aperto/bloccato), la lettera del drive ed il percorso completo del vault. La tabella nella parte inferiore mostra il contenuto del vault selezionato.

23.2.1. Creare un Vault

Per creare un nuovo vault, utilizzare uno di questi metodi:

- Cliccare su **Creare vault**.
- Fare clic con il tasto destro nella tabella dei vault e selezionare **Crea**.
- Fare clic con il pulsante destro sul desktop o su una cartella del computer, puntare su **Criptazione File Acronis Backup and Security** e selezionare **Crea**.

Apparirà una nuova finestra.

Crea File Vault

Procedere come segue:

1. Specificare la posizione ed il nome del vault.
   - Cliccare su **Sfoglia**, selezionare la posizione del vault e salvare il file sotto il nome desiderato.
   - È sufficiente digitare il nome del vault nel campo corrispondente per crearlo in Documenti. Per aprire i Documenti, fare clic su start menu Start di Windows e poi **Documenti**.
   - Digitare il percorso completo del vault sul disco. Ad esempio, `C:\my_vault.bvd`.
2. Scegliere una lettera dal menu per il drive. Quando aprite il vault, un disco virtuale con la lettera selezionata apparirà su Risorse del Computer.
3. Digitare la password desiderata per il vault nei campi **Password** e **Conferma**. Qualsiasi persona che tenti di aprire il vault ed accedere ai suoi file, dovrà fornire la password.
4. Selezionare **Formattare drive** per formattare il disco virtuale assegnato al vault. È necessario formattare l'unità prima che si possa aggiungere file al vault.
5. Se desiderate cambiare la dimensione predefinita del vault (50 MB), digitare il valore desiderato nel campo **Dimensione del Vault**.
6. Cliccare su **Creare** se desiderate creare solo il vault nella destinazione selezionata. Per creare e mostrare il vault come un disco virtuale nelle Risorse del Computer, cliccare su **Creare & Aprire** .

Acronis Backup and Security 2010 informerà immediatamente sul risultato dell'operazione. Se si verifica un errore, utilizzare il messaggio di errore per risolvere l'errore. Selezionare **OK** per chiudere la finestra.

Nota

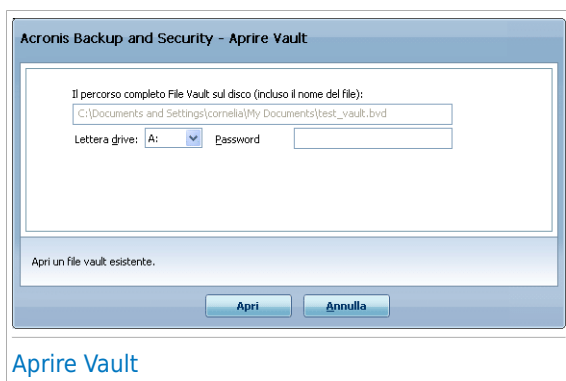
Potrebbe essere conveniente salvare tutti i file vault nella stessa posizione. In questo modo, è possibili trovarli più velocemente.

23.2.2. Aprire un Vault

Per accedere e lavorare sui file immagazzinati in un vault, dovrete aprire il vault. Quando aprite un vault, apparirà un disco virtuale nelle Risorse del Computer. Il drive avrà la lettera di disco assegnata al vault.

Per aprire un vault, utilizzare uno di questi metodi:

- Selezionare il vault dalla tabella e cliccare su **Aprire vault**.
- Fare clic con il pulsante destro sul vault nella tabella e selezionare **Apri**.
- Fare clic con il pulsante destro sul vault nel computer, puntare su **Criptazione File Acronis Backup and Security** e selezionare **Apri**.

Apparirà una nuova finestra.

Aprire Vault

Procedere come segue:

1. Scegliere una lettera dal menu per il drive.
2. Digitare la password per il vault nel campo **Password**.
3. Cliccare **Aprire**.

Acronis Backup and Security 2010 informerà immediatamente sul risultato dell'operazione. Se si verifica un errore, utilizzare il messaggio di errore per risolvere l'errore. Selezionare **OK** per chiudere la finestra.

23.2.3. Bloccare un Vault

Quando abbiate finito di lavorare in un vault, dovrete bloccarlo per proteggere i vostri dati. Bloccando la vault, l'unità disco virtuale corrispondente sparisce da

Risorse del computer. Di conseguenza l'accesso ai dati archiviati nel vault è completamente bloccato.

Per bloccare un vault, utilizzare uno di questi metodi:

- Selezionare il vault nella tabella e cliccare su **Bloccare vault**.
- Fare clic con il pulsante destro sul vault nella tabella e selezionare **Blocca**.
- Fare clic con il pulsante destro sul disco virtuale corrispondente da Risorse del Computer, puntare su **Criptazione File Acronis Backup and Security** e selezionare **Blocca**.

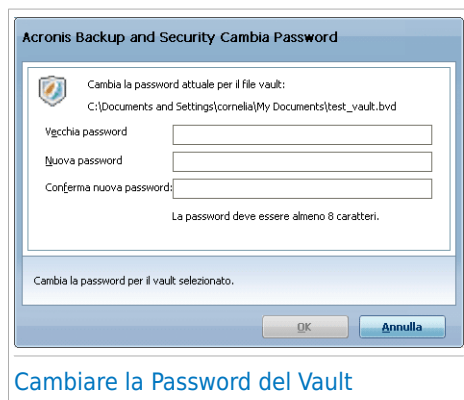
Acronis Backup and Security 2010 informerà immediatamente sul risultato dell'operazione. Se si verifica un errore, utilizzare il messaggio di errore per risolvere l'errore. Selezionare **OK** per chiudere la finestra.

23.2.4. Cambiare la Password del Vault

Il vault deve essere bloccato prima che si possa cambiare la sua password. Per cambiare la password di un vault, utilizzare uno di questi metodi:

- Selezionare il vault nella tabella e cliccare su **Cambiare password**.
- Fare clic con il pulsante destro sul vault nella tabella e selezionare **Cambia password**.
- Fare clic con il pulsante destro sul vault sul computer, puntare su **Acronis Backup and Security File Vault** e selezionare **Cambia la password del vault**.

Apparirà una nuova finestra.

Cambiare la Password del Vault

Procedere come segue:

1. Digitare la password corrente del vault nel campo **Vecchia password**.

2. Digitare la nuova password del vault nei campi **Nuova password** e **Confermare nuova password**.

Nota

La password deve essere composta da almeno 8 caratteri. Per avere una password forte, utilizzare una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, $ o @).

3. Cliccare su **OK** per cambiare la password.

Acronis Backup and Security 2010 informerà immediatamente sul risultato dell'operazione. Se si verifica un errore, utilizzare il messaggio di errore per risolvere l'errore. Selezionare **OK** per chiudere la finestra.

23.2.5. Aggiungere dei File ad un Vault

Per aggiungere dei file ad un vault, seguire questi passaggi:

1. Seleziona dalla tabella vault il vault a cui si desidera aggiungere file.
2. Se il vault è bloccato, prima bisogna aprirlo (facendo clic con il pulsante destro e selezionando **Apri vault**).
3. Cliccare su **Aggiungere file**. Apparirà una nuova finestra.
4. Selezionare i file / cartelle che volete aggiungere al vault.
5. Cliccare **OK** per copiare gli oggetti selezionati nel vault.

Una volta che il vault è aperto, è possibile utilizzare direttamente l'unità disco virtuale corrispondente al vault. Attenersi alla seguente procedura:

1. Aprire Documenti (fare clic su start menu Start di Windows e poi **Risorse del computer**).
2. Inserire l'unità disco virtuale corrispondente al vault. Cercare la lettera dell'unità assegnata al vault quando lo si è aperto.
3. Copia e incolla e trascina file e cartelle direttamente a questa unità disco virtuale.

23.2.6. Rimuovere dei File da un Vault

Per rimuovere un file da un vault, seguire questi passaggi:

1. Selezionare dalla tabella dei vault quello contenente il file da rimuovere.
2. Se il vault è bloccato, prima bisogna aprirlo (facendo clic con il pulsante destro e selezionando **Apri vault**).
3. Selezionare il file da rimuovere dalla tabella che mostra il contenuto del vault.
4. Fare clic su **Elimina file/cartelle**.

Se il vault è aperto, potrete rimuovere direttamente i file dal disco virtuale assegnato al vault. Attenersi alla seguente procedura:

1. Aprire Documenti (fare clic su start menu Start di Windows e poi **Risorse del computer**).
2. Inserire l'unità disco virtuale corrispondente al vault. Cercare la lettera dell'unità assegnata al vault quando lo si è aperto.
3. Rimuove file o cartelle come si fa normalmente in Windows (ad esempio, fare clic con il pulsante destro su un file che si vuole eliminare e selezionare **Elimina**).

24. Modalità Gioco / Portatile

La Modalità Gioco / Portatile vi permette di configurare le modalità speciali di operatività di Acronis Backup and Security 2010:

- Modalità Gioco modifica temporaneamente le impostazioni del prodotto in modo di minimizzare il consumo di risorse mentre giocate.
- Modalità Portatile impedisce che le funzioni programmate vengano eseguite quando il portatile funziona con la batteria in modo da risparmiare energia della batteria.

24.1. Modalità giochi

La Modalità Gioco modifica temporaneamente le impostazioni di protezione in modo di minimizzare l'impatto sulle prestazioni del sistema. Mentre siete in Modalità Gioco, verranno applicate le seguenti impostazioni:

- Tutti gli allarmi e pop-up Acronis Backup and Security 2010 sono disabilitati.
- Il livello di protezione in tempo reale di Acronis Backup and Security 2010 è impostato come **Permissivo**.
- Il Firewall di Acronis Backup and Security 2010 è impostato con **Consentire tutti**. Questo significa che tutte le nuove connessioni (sia in entrata che in uscita) vengono consentite, indipendentemente della porta o protocollo utilizzati.
- Gli aggiornamenti non vengono eseguiti di default.

Nota

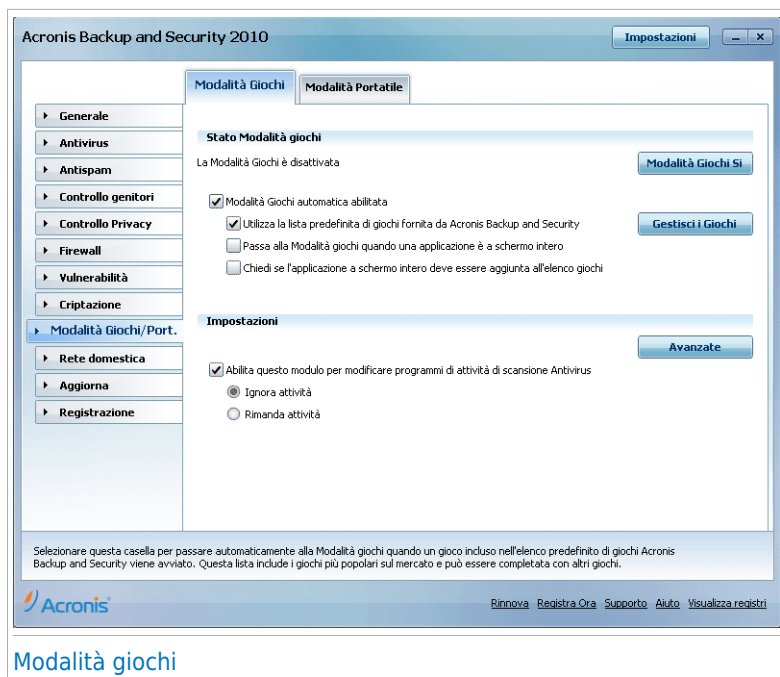
Per cambiare queste impostazioni, cliccare su Aggiornamento > Impostazioni e deselezionare la casella **Non aggiornare se la Modalità Gioco è attiva**.

- Le funzioni di scansione programmate sono disabilitate di default.

Di default, Acronis Backup and Security 2010 entra automaticamente in Modalità Gioco quando iniziate un gioco incluso nella lista dei giochi conosciuti o quando un'applicazione passa a schermo pieno. Potete entrare manualmente in Modalità Gioco usando la hotkey di default `Ctrl+Alt+Shift+G`. E' fortemente consigliato di uscire dalla Modalità Gioco quando avete finito di giocare (potete usare la stessa hotkey di default `Ctrl+Alt+Shift+G`).

Nota

Mentre siete in Modalità Gioco, potete vedere la lettera G sull'icona Acronis .

Per configurare la Modalità Gioco, andare su **Modalità Gioco / Laptop>Modalità Gioco** in Modalità Avanzata.

Modalità giochi

Nella parte superiore della sezione è possible vedere lo stato della Modalità Gioco. È possibile fare clic su **Attiva Modalità giochi** o **Disattiva Modalità giochi** per cambiare lo stato attuale.

24.1.1. Configurazione Automatica della Modalità Gioco

La Modalità Gioco automatica consente a Acronis Backup and Security 2010 di entrare in Modalità Gioco quando un gioco viene rilevato. E' possibile configurare le seguenti opzioni:

- **Usare la lista di default dei giochi fornita da Acronis Backup and Security** - per entrare automaticamente in Modalità Gioco quando iniziate un gioco della lista dei giochi conosciuti da Acronis Backup and Security 2010. Per vedere questo elenco, fare clic su **Gestione giochi** e quindi su **Elenco giochi**.
- **Entrare nella Modalità giochi quando una applicazione è a schermo pieno** - per entrare automaticamente nella Modalità giochi quando un'applicazione passa a schermo pieno.
- **Aggiungere l'applicazione alla lista dei giochi?** - perchè vi venga richiesto di aggiungere una nuova applicazione alla lista dei giochi quando abbandonate lo schermo pieno. Aggiungendo una nuova applicazione alla lista dei giochi, la

prossima volta che la avvierete Acronis Backup and Security 2010 entrerà automaticamente in Modalità Gioco.

Nota

Se non desiderate che Acronis Backup and Security 2010 entri automaticamente in Modalità Gioco, deselezionare la casella **Modalità Gioco Automatica**.

24.1.2. Gestione della Lista dei Giochi

Acronis Backup and Security 2010 entra automaticamente in Modalità Gioco quando avviate una applicazione dalla lista dei giochi. Per visualizzare e gestire la lista dei giochi, cliccare su **Gestire Giochi**. Apparirà una nuova finestra.

Lista dei Giochi

Nuove applicazioni vengono automaticamente aggiunte alla lista quando:

- Avviate un gioco dalla lista dei giochi conosciuti di Acronis Backup and Security 2010. Per visualizzare la lista, fare clic su **Elenco giochi**.
- Dopo aver abbandonato lo schermo pieno, aggiungete l'applicazione alla lista dei giochi dalla finesta proposta.

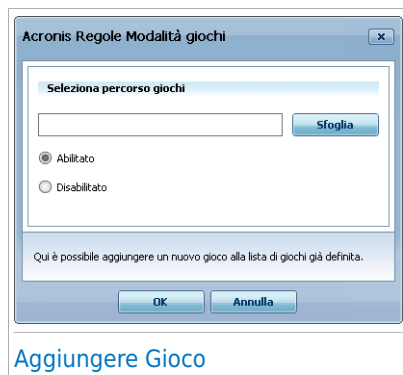
Se volete disabilitare la Modalità Gioco Automatica per un'applicazione specifica della lista, deselezionare la casella corrispondente. Dovreste disabilitare la Modalità Gioco Automatica per le applicazioni regolari che vanno in schermo pieno, come web browser o movie player.

Per gestire questa lista giochi, potete usare i tasti situati nella parte superiore della tabella:

- Cliccare su **OK** per aggiungere la nuova applicazione alla lista dei giochi.

- **Rimuovi** - per rimuovere tutte le applicazioni installate.
- Cliccare su **OK** per aggiungere l'applicazione alla lista dei giochi.

Aggiungere o Modificare Giochi

Quando aggiungete o modificate un'entrata della lista dei giochi, apparirà la seguente finestra:

Aggiungere Gioco

Cliccare su **Sfoglia** per selezionare l'applicazione o digitare il percorso completo dell'applicazione nel campo corrispondente.

Se non si desidera entrare automaticamente in Modalità Gioco quando l'applicazione è già iniziata, selezionare **Disabilitare**.

Cliccare su **OK** per aggiungere l'entrata alla lista dei giochi.

24.1.3. Configurazione delle Impostazioni della Modalità Gioco

Per configurare il comportamento delle funzioni programmate, usare queste opzioni:

- **Abilitare questo modulo per modificare le programmazioni attività scansione antivirus** - per impedire che attività di scansione programmate vengano eseguite mentre si è nella Modalità giochi. E' possibile selezionare una delle seguenti opzioni:

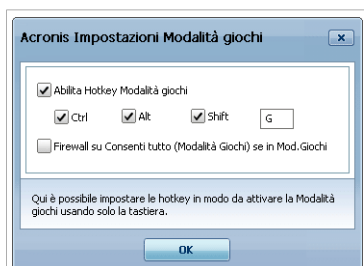
Opzione	Descrizione
Saltare Task	Non eseguire la funzione programmata.
Posporre Task	Eseguire la funzione programmata immediatamente dopo che siete usciti dalla Modalità Gioco.

Per disabilitare automaticamente il Firewall Acronis Backup and Security 2010e quando vi troviate in Modalità Gioco, seguire questi passaggi:

1. Cliccare su **Impostazioni Avanzate**. Apparirà una nuova finestra.
2. Selezionare la casella di controllo **Imposta Firewall su Consenti tutto (Modalità giochi) quando in Modalità giochi**.
3. Selezionare **Applica** per salvare le modifiche.

24.1.4. Modifica Hotkey della Modalità Gioco.

Potete entrare manualmente in Modalità Gioco usando la hotkey di default `Ctrl+Alt+Shift+G`. Per modificare la hotkey, seguire questi passaggi:

1. Cliccare su **Impostazioni Avanzate**. Apparirà una nuova finestra.

Avanzate

2. Sotto l'opzione **Usare HotKey**, impostare la hotkey desiderata:
   - Scegliere i tasti di modifica che si vogliono usare selezionando uno dei seguenti: tasto Control (`Ctrl`), tasto Maiuscola (`Shift`) o tasto Alternare (`Alt`).
   - Nel campo editabile, inserire la lettera corrispondente al tasto regolare che si vuole usare.

   Ad esempio, se volete usare la hotkey `Ctrl+Alt+D`, dovete solo controllare i tasti `Ctrl` e `Alt` ed inserire la `D`.

   Nota
   Deselezionare la casella **Usare HotKey** disabiliterà la hotkey.

3. Selezionare **Applica** per salvare le modifiche.

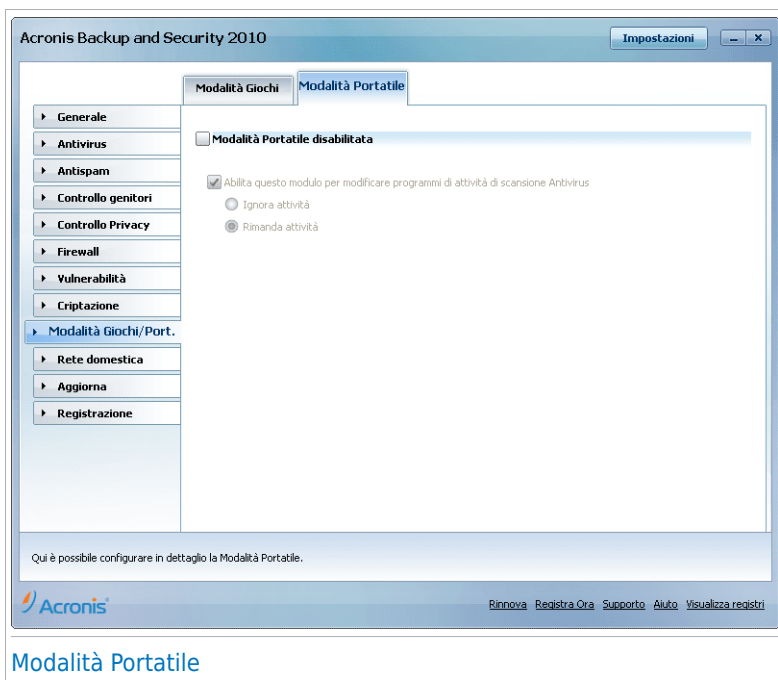
24.2. Modalità Portatile

La Modalità Portatile è stata specialmente disegnata per chi usa i laptop/notebook. Il suo proposito è minimizzare l'impatto di Acronis Backup and Security 2010 sul consumo di energia mentre questi apparecchi funzionino con la batteria.

Mentre siete in Modalità Portatile, le funzioni programmate non verranno eseguite di default.

Acronis Backup and Security 2010 rileva quando il vostro portatile sta funzionando con la batteria ed automaticamente va in Modalità Portatile. Nello stesso modo, Acronis Backup and Security 2010 uscirà automaticamente dalla Modalità Portatile quando rileverà che il portatile non sta più lavorando con la batteria.

Per configurare la Modalità Portatile, andare su **Modalità Gioco / Portatile>Modalità Portatile** in Modalità Avanzata.

Modalità Portatile

Potete vedere se la Modalità Portatile è abilitata o meno. Se la Modalità Portatile è abilitata, Acronis Backup and Security 2010 applicherà le impostazioni configurate mentre il portatile lavora con la batteria.

24.2.1. Configurazione delle Impostazioni della Modalità Portatile

Per configurare il comportamento delle funzioni programmate, usare queste opzioni:

- **Abilitare questo modulo per modificare le programmazioni attività scansione antivirus** - per impedire che attività di scansione programmate vengano eseguite mentre si è nella Modalità portatile. E' possibile selezionare una delle seguenti opzioni:

Opzione	Descrizione
Saltare Task	Non eseguire la funzione programmata.
Posporre Task	Eseguire la funzione programmata immediatamente dopo che siete usciti dalla Modalità Portatile.

25. Rete domestica

Il modulo Rete vi permette gestire i prodotti Acronis installati sui computer di casa da un singolo computer.

Importante

Può gestire solo i seguenti prodotti di sicurezza Acronis:

- Acronis AntiVirus 2010
- Acronis Internet Security Suite 2010
- Acronis Backup and Security 2010

Mappa di rete

Per essere in grado di gestire i prodotti Acronis installati sui computer di casa, dovete seguire questi passaggi:

1. Unirvi alla rete domestica Acronis sul vostro computer. Unirsi alla rete consiste in configurare una password di amministrazione per la gestione della rete domestica.
2. Andare su ogni computer che si vuole gestire ed aggiungerli alla rete (impostare la password).

3. Tornare al vostro computer ed aggiungere i computer che volete gestire.

25.1. Unirsi alla Rete Acronis

Per unirsi alla rete domestica Acronis, seguire questi passaggi:

1. Fare clic su **Abilita rete**. Vi verrà chiesto di configurare le password per la gestione domestica.

Configurare Password

2. Inserire la stessa password in ognuno dei campi corrispondenti.
3. Selezionare **OK**.

Potete vedere il nome del computer apparire nella mappa della rete.

25.2. Aggiungere dei computer alla Rete Acronis

Prima di poter aggiungere un computer alla rete domestica Acronis dovrete configurare la password per la gestione domestica Acronis sul rispettivo computer.

Per aggiungere un computer alla rete domestica Acronis , seguire questi passi:

1. Fare clic su **Aggiungi Computer**. Vi verrà chiesto di fornire la password per la gestione domestica locale.

Inserire Password

2. Digitare la password per la gestione domestica e cliccare su **OK**. Apparirà una nuova finestra.

Aggiungi Computer

Potete vedere l'elenco dei computer in questa rete. Il significato dell'icona è il seguente:

Indica un computer online senza prodotti Acronis gestibile installati.

Indica un computer online con un prodotto di Acronis gestibile installato.

Indica un computer offline con un prodotto di Acronis gestibile installato.

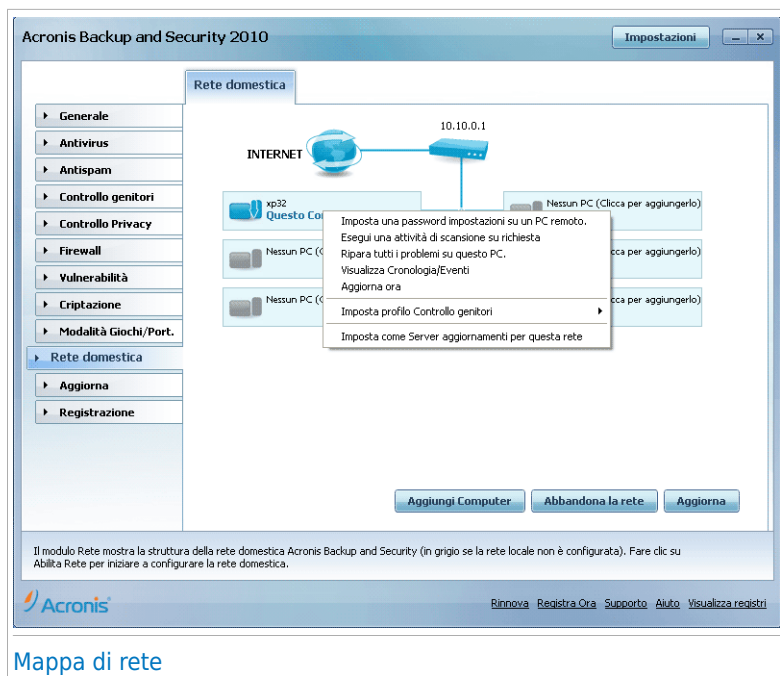
3. Eseguire una delle seguenti azioni:
   - Selezionare dall'elenco il nome del computer da aggiungere.
   - Digitare l'indirizzo IP o il nome del computer da aggiungere nel campo corrispondente.
4. Selezionare **Aggiungi**. Vi verrà chiesto di fornire la password per la gestione domestica sul rispettivo computer.

Autenticare

5. Digitare la password per la gestione domestica configurata sul rispettivo computer.
6. Selezionare **OK**. Se avete fornito la password corretta, il nome del computer selezionato apparirà nella mappa di rete.

Nota
Potete aggiungere fino a cinque computer alla mappa di rete.

25.3. Gestione della Rete Acronis

Una volta che avete creato con successo una rete domestica Acronis, potrete gestire tutti i prodotti Acronis da un singolo computer.

Mappa di rete

Se muovete il cursore su un computer nella mappa di rete, potete vedere una breve informazione su di esso (nome, indirizzo IP, numero di problemi che colpiscono la sicureza del sistema).

Se si fa clic sul nome di un computer nella mappa di rete, è possibile vedere tutte le funzioni di amministrazione che si possono eseguire sul computer remoto.

- **Rimuovi il PC dalla rete domestica**

  Permette di rimuovere il PC dalla rete.

- **Stabilire una password per le impostazioni su un PC remoto**

  Permette di creare una password per limitare l'accesso alle impostazioni Acronis sul PC.

- **Eseguire una attività di scansione su richiesta**

  Permette di eseguire una scansione a richiesta sul computer remoto. E' possibile compiere una qualsiasi delle seguenti attività di scansione: Scansione Documenti, Scansione del Sistema o Scansione del Sistema Approfondita.

- **Risolvere tutti i problemi su questo computer**

Permette di risolvere i problemi che influenzano la sicurezza del computer seguendo l'assistente Risolvi tutto.

- **Visualizzare Cronologia/Eventi**

  Permette di accedere al modulo **Cronologia&Eventi** del prodotto Acronis installato sul computer.

- **Aggiorna adesso**

  Avvia il processo di aggiornamento per il prodotto Acronis installato sul computer.

- **Imposta Profilo Controllo genitori**

  Permette di impostare la categoria di età da utilizzare per il filtro web del Controllo Genitori del computer: bambino, adolescente o adulto.

- **Impostare come Server di aggiornamento per questa rete**

  Permette di impostare il computer come server di aggiornamento per tutti i prodotti Acronis installati sui computer della rete. Utilizzando questa opzione si ridurrà il traffico Internet, poiché un solo computer della rete si collegherà ad Internet per scaricare gli aggiornamenti.

Prima di eseguire una funzione su un particolare computer, vi verrà chiesto di fornire la password per la gestione domestica locale.

Inserire Password

Digitare la password per la gestione domestica e cliccare su **OK**.

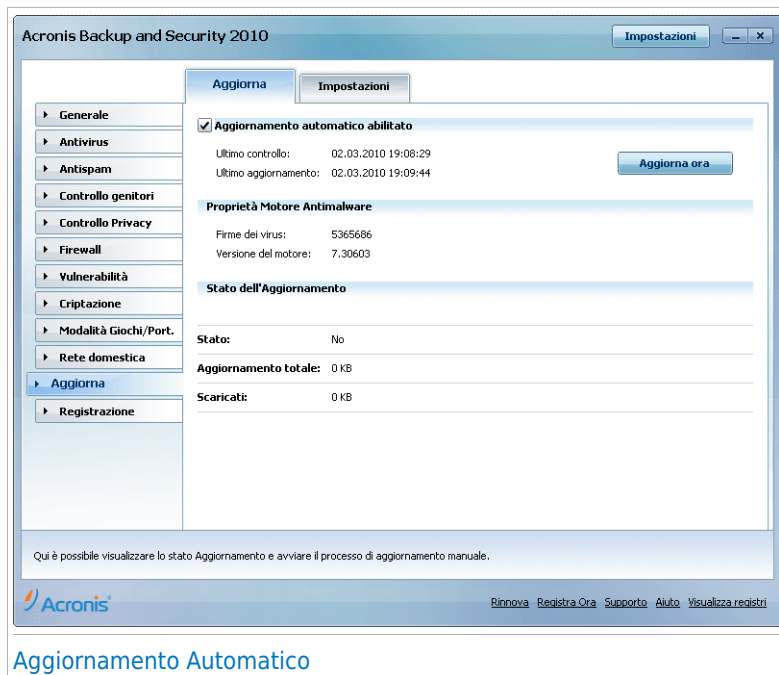
Nota

Se programmate di eseguire più funzioni, potete selezionare **Non mostrare di nuovo questo messaggio durante questa sessione**. Selezionando questa opzione non vi verrà più chiesta la password durante la sessione corrente.

26. Aggiorna

Tutti giorni vengono trovati ed identificati nuovi malware. E' quindi molto importante mantenere aggiornato il vostro Acronis Backup and Security 2010 con le impronte più recenti del malware.

Se siete connessi ad Internet con banda larga o DSL, Acronis Backup and Security 2010 si prenderà cura di sè da solo. Per default, esso cercherà degli aggiornamenti, ogni volta che avvierete il vostro computer ed ogni **ora**dopo l'avvio.

Se viene rilevato un aggiornamento, vi verrà chiesto di confermare l'aggiornamento o l'aggiornamento verrà eseguito automaticamente, a seconda delle impostazioni dell'aggiornamento automatico update settings.

Il processo di aggiornamento viene eseguito involo, il chè vuol dire che i file da aggiornare vengono sostituiti progressivamente. In questo modo, il processo di aggiornamento non interesserà l'operatività del prodotto, nello stesso tempo, ogni vulnerabilità verrà esclusa.

Gli Aggiornamenti arrivano nei seguenti modi:

- **Aggiornamenti per motori Antivirus** - non appena compaiono nuove minacce, i file contenenti le impronte dei virus devono essere aggiornati per garantire una protezione aggiornata permanente contro queste nuove minacce. Questo tipo di aggiornamento è anche conosciuto come **Virus Definitions Update**.
- **Aggiornamenti per motori Antispam** - verranno aggiunte nuove regole ai filtri euristico ed URL, e nuove immagini al filtro immagini. Ciò contribuirà ad aumentare l'efficacia del vostro motore Antispam. Questo tipo di aggiornamento è anche conosciuto come **Antispam Update**.
- **Aggiornamento per I motori antispyware** - nuove firme antispyware saranno aggiunte al database. Questo tipo di aggiornamento è anche conosciuto come **Antispyware Update**.
- **Aggiornamenti del Prodotto** - quando viene rilasciata la nuova versione di un prodotto, vengono introdotte nuove funzionalità e tecniche di scansione al fine di migliorare l'efficienza del prodotto. Questo tipo di aggiornamento è anche conosciuto come **Product Update**.

26.1. Aggiornamento Automatico

Per visualizzare informazioni relative all'aggiornamento ed eseguire aggiornamenti automatici, fare clic su **Aggiornamento>Aggiornamento** in Modalità Avanzata.

Aggiornamento Automatico

Qui è possibile visualizzare quando sono stati eseguiti l'ultimo controllo degli aggiornamenti e l'ultimo aggiornamento, così come le informazioni sull'ultimo aggiornamento eseguito (se con successo o gli errori verificatisi). Inoltre si mostrano informazioni sulla versione del motore corrente ed il numero di impronte.

se aprite questa sezione durante un aggiornamento potrete visualizzare lo stato del download.

Importante

Per essere sempre protetti, tenete l' **Aggiornamento Automatico** abilitato.

26.1.1. Richiedere un aggiornamento

L’aggiornamento automatico può essere eseguito in qualsiasi momento, cliccando su **Aggiornare adesso**. Questo aggiornamento è conosciuto anche come **Aggiornamento su richiesta dell’utente**.

Il modulo **Aggiornamento** si collegherà al server di aggiornamento di Acronis e verificherà la disponibilità. Se viene rilevato un aggiornamento, secondo le opzioni impostate nella sezione Impostazioni Aggiornamento Manuale, vi verrà chiesto di confermarlo oppure verrà eseguito automaticamente.

Importante
Può essere necessario riavviare il computer una volta completato l'aggiornamento. Noi consigliamo di farlo al più presto possibile.

Nota
Se siete connessi a Internet mediante una connessione telefonica, è consigliato l'aggiornamento periodico di Acronis Backup and Security 2010 su richiesta dell'utente.

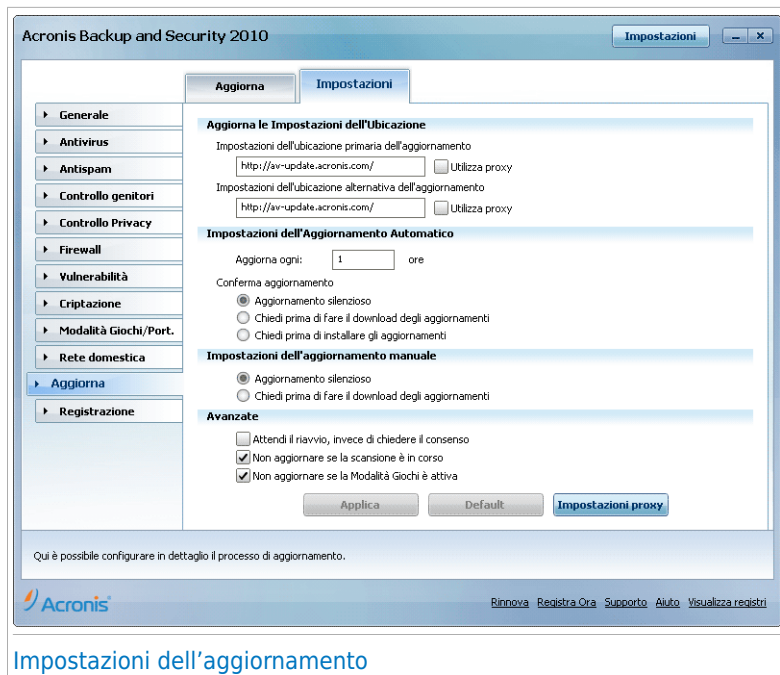
26.1.2. Disattivare Aggiornamento Automatico

Scegliendo di disattivare l'aggiornamento automatico, apparirà una finestra di avviso. Dovete confermare la vostra scelta selezionando dal menu per quanto tempo volete che l'aggiornamentop automatico venga disattivato. Potete disattivare l'aggiornamento automatico per 5, 15 o 30 minuti, per un'ora, permanentemente o fino al riavvio del sistema.

Avvertimento
Questa è una questione critica di sicurezza. Vi consigliamo di disattivare l'aggiornamento automatico per il minimo tempo possibile. Se Acronis Backup and Security 2010 non verrà aggiornato regolarmente non sarà in grado di proteggervi dalle minacce più recenti.

26.2. Impostazioni dell'aggiornamento

Gli aggiornamenti possono essere eseguiti dalla rete locale, su Internet, direttamente o attraverso un server proxy. Per default, Acronis Backup and Security 2010 controllerà la disponibilità di aggiornamenti ogni ora sulla Internet ed installerà gli aggiornamenti disponibili senza avvisarvi.

Per configurare le impostazioni di aggiornamento e gestire i proxy, fare clic su **Aggiornamento>Impostazioni** in Modalità Avanzata.

Impostazioni dell'aggiornamento

Le impostazioni dell'aggiornamento sono ragruppate in 4 categorie (**Impostazioni Ubicazione Aggiornamento**, **Impostazioni Aggiornamento Automatico**, **Impostazioni Aggiornamento Manuale** ed **Impostazioni Avanzate**). Ogni categoria verrà descritta separatamente.

26.2.1. Impostare Ubicazioni Aggiornamento

Per configurare le ubicazioni dell'aggiornamento utilizzare le opzioni della categoria **Impostazioni Ubicazione Aggiornamento**.

Importante

Configurare queste impostazioni solo se siete connessi ad una rete locale che immagazzini localmente le impronte malware di Acronis o se vi connettete ad Internet attraverso un server proxy.

Per modificare una delle ubicazioni dell'aggiornamento, inserire l'URL dello specchio locale nel campo **URL** corrispondente all'ubicazione che si desidera modificare.

Nota
Vi consigliamo di impostare come ubicazione principale dell'aggiornamento lo specchio locale e di non modificare l'ubicazione alternativa, come piano di sicurezza interna nel caso in cui lo specchio locale non fosse disponibile.

Nel caso in cui l'azienda usi un server proxy per connettersi ad internet, selezionare **Usa proxy** e poi fare clic su **Impostazioni proxy** per configurare le impostazioni proxy. Per ulteriori informazioni, vi preghiamo di riferirvi a *«Gestione Proxies»* (p. 264)

26.2.2. Configurazione Aggiornamento Automatico

Per configurare l'esecuzione automatica del processo di aggiornamento da parte di Acronis Backup and Security 2010, utilizzare le opzioni della categoria **Impostazioni Aggiornamento Automatico**.

È possibile specificare il numero di ore tra due controlli consecutivi per aggiornamenti nel campo **Aggiorna ogni**. Per default l'intervallo di tempo tra aggiornamenti è impostato ad un'ora.

Per specificare come dovrebbe essere eseguito il processo di aggiornamento automatico, selezionare una delle seguenti opzioni:

- **Aggiornamento silenzioso** - Acronis Backup and Security 2010 scarica ed implementa l'aggiornamento automaticamente.
- **Chiedere prima di scaricare gli aggiornamenti** - ogni volta che un aggiornamento è disponibile, vi verrà richiesto se eseguire il download.
- **Chiedere prima di installare gli aggiornamenti** - ogni volta che si scarica un aggiornamento, vi verrà richiesto se installarlo.

26.2.3. Configurazione Aggiornamento Manuale

Per specificare come dovrà essere eseguito l'aggiornamento manuale (aggiornamento a richiesta dell'utente) selezionare una delle seguenti opzioni dalla categoria **Impostazioni Aggiornamento Manuali**:

- **Aggiornamento silenzioso** - l'aggiornamento manuale verrà eseguito automaticamente in background, senza l'intervento dell'utente.
- **Chiedere prima di scaricare gli aggiornamenti** - ogni volta che un aggiornamento è disponibile, vi verrà richiesto se eseguire il download.

26.2.4. Configurazione delle Impostazioni Avanzate

Per evitare che il processo di aggiornamento di Acronis interferisca con il vostro lavoro, configurare le opzioni nella categoria **Impostazioni Avanzate**:

- **Attendi conferma prima di riavviare** - Se un aggiornamento richiede un riavvio, il prodotto continuerà a lavorare con i vecchi file finché il sistema venga riavviato.

Non verrà chiesto all'utente di riavviare, a fin che il processo di aggiornamento non interferisca con il lavoro dell'utente.

- **Non aggiornare se la scansione è attiva** - Acronis Backup and Security 2010 non verrà aggiornato se è in corso un processo di scansione. In tal modo la procedura di aggiornamento Acronis Backup and Security 2010 non interferisce con le operazioni di scansione.

Nota
Se Acronis Backup and Security 2010 è aggiornato durante una scansione, la procedura di scansione viene interrotta.

- **Non aggiornare se la modalità gioco è attiva** - Acronis Backup and Security 2010 non eseguirà l'aggiornamento se la modalità gioco è attiva. In questo modo si può minimizzare l'influenza del prodotto sulla performance del vostro sistema durante i giochi.

26.2.5. Gestione Proxies

Se la vostra azienda utilizza un server proxy per connettersi ad Internet, dovrete specificare le impostazioni di proxy perchè Acronis Backup and Security 2010 si possa aggiornare da solo. Altrimenti, esso utilizzerà le impostazioni proxy dell'amministratore che installò il prodotto o, se ci sono, le impostazioni predefinite del browser dell'utente corrente.

Nota
Le impostazioni del proxy possono essere configurate solo da utenti con diritti di amministratore sul computer oppure da "power users" (utenti che conoscono la password per le impostazioni del prodotto).

Per gestire le impostazioni proxy, fare clic su **Impostazioni Proxy**. Apparirà una nuova finestra.

Gestore del proxy

Vi sono tre gruppi di impostazioni del proxy:

- **Proxy rilevato al momento dell'installazione)** - impostazioni del proxy rilevate sull'account dell'amministratore durante l'installazione le quali possono essere configurate solo utilizzando tale account. Se il server proxy richiede un nome utente ed una password, specificarli nei rispettivi campi.
- **Proxy del browser predefinito** - impostazioni proxy dell'utente attuale, tratte dal browser predefinito. Se il server proxy richiede un nome utente e una password, è necessario specificarle nei campi corrispondenti.

Nota

I browser web supportati sono Internet Explorer, Mozilla Firefox ed Opera. Se usate un altro browser di default, Acronis Backup and Security 2010 non sarà in grado di ottenere le impostazioni del proxy dell'utente corrente.

- **Proxy personalizzato** - impostazioni del proxy che si possono configurare se si accede come amministratore.

  Le seguenti impostazioni devono essere specificate:
  - **Indirizzo** - inserire l'IP del server proxy.
  - **Porta** - inserire la porta che utilizza Acronis Backup and Security 2010 per connettersi al server proxy.
  - **Nome Utente** - inserire un nome utente riconosciuto dal proxy.

- **Password** - inserire la password valida per l’utenza, già specificata precedentemente.

Quando ci si tenta di connettere ad Internet, ogni set di impostazione del proxy viene tentato uno alla volta, finchè Acronis Backup and Security 2010 non riesce a connettersi.

In primo luogo verrà usato il set contenente le vostre impostazioni per connettersi ad Internet. Se questo non funzionasse, verranno utilizzate successivamente le impostazioni del proxy rilevate al momento dell'installazione. Ed infine, se neanche queste funzionassero, le impostazioni del proxy dell'utente corrente verranno ricavate dal browser predefinito ed utilizzate per connettersi ad Internet.

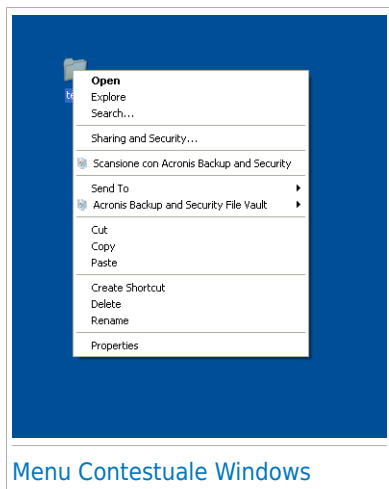
Selezionare **OK** per salvare le modifiche e chiudere la finestra.

Selezionare **Applica** per salvare le modifiche oppure selezionare **Preimpostazione** per tornare alle impostazioni di default.

Integrazione in Software Windows e di terzi

27. Integrazione nel Menu Contestuale Windows

Il menu contestuale Windows appare ogni volta che si fa clic con il pulsante destro su un file o una cartella del computer o un oggetto sul desktop.

Menu Contestuale Windows

Acronis Backup and Security 2010 si integra nel menu contestuale Windows per aiutare a scansionare facilmente file alla ricerca di virus e prevenire altri utenti da accedere ai file privati. È possibile individuare velocemente opzioni Acronis Backup and Security 2010 sul menu contestuale cercando l'icona Acronis.

- Scansiona con Acronis Backup and Security
- Acronis Backup and Security File Vault

27.1. Scansiona con Acronis Backup and Security

È semplice eseguire la scansione di file, cartelle e persino dischi rigidi interi utilizzando il menu contestuale Windows. Fare clic con il pulsante destro del mouse sull'oggetto che si desidera scansionare e selezionare dal menu **Scansiona con Acronis Backup and Security**. La procedura guidata di Scansione apparirà e vi guiderà attraverso il processo di scansione.

Opzioni di scansione. Le opzioni di scansione sono preconfigurate per i migliori risultati di scansione. Se vengono individuati fili infetti, Acronis Backup and Security 2010 cercherà di disinfettarli (rimuovere il codice malware). Se la disinfettazione non riesce, la procedura guidata Antivirus Scan consentirà di specificare altre azioni da intraprendere sui file infetti.

Per modificare le opzioni di scansione, seguire questi passaggi:

1. Aprire Acronis Backup and Security 2010 e passare l'interfaccia utente in Modalità Avanzata.
2. Clicca su **Antivirus** dal menù a sinistra.
3. Fare clic sulla scheda **Scansione Virus**.
4. Fare clic con il tasto destro sull'attività **Scansione contestuale** e selezionare **Apri**. Apparirà una finestra.
5. Fare clic su **Personalizza** e configurare le opzioni di scansione come necessario. Per scoprire cosa fa una opzione, posizionare il mouse su di essa e leggere la descrizione visualizzato nel fondo della finestra.
6. Selezionare **Applica** per salvare le modifiche.
7. Fare clic su **OK** per confermare e applicare le nuove opzioni di scansione.

Importante

Non si dovrebbero modificare le opzioni di scansione di questo metodo di scansione a meno che non vi siano ragioni valide per farlo.

27.2. Acronis Backup and Security File Vault

Acronis Backup and Security File Vault aiuta ad archiviare in modo sicuro i documenti confidenziali sul computer tramite l'uso di file vault.

- Il file vault è uno spazio sicuro dove immagazzinare informazioni personali o file sensibili.
- Il file vault è un file criptato sul vostro computer con estensione `bvd`. Siccome è criptato, i dati al suo interno sono invulnerabili a furti o a violazioni di sicurezza.
- Quando aprite questo file `bvd`, apparirà una nuova partizione logica (un nuovo drive). Vi sarà più facile capire questo processo se pensate ad uno simile: aprire un'immagine ISO come CD virtuale.

  Aprire Risorse del Computer e vedrete un nuovo drive basato sulla vostra criptazione file. In esso sarete in grado di fare operazioni sui file (copiare, cancellare, modificare, etc). I file saranno protetti finchè risiederanno in questo drive (perchè viene richiesta una password per l'operazione di apertura).

  Quando avrete finito, bloccare (smontare) il file per comminciare a proteggere il suo contenuto.

È possibile individuare facilmente file vault Acronis Backup and Security 2010 sul computer tramite l'icona Acronis e l'estensione `.bvd`.

Nota

Questa sezione mostra come creare e gestire file vault Acronis Backup and Security 2010 usando solo opzioni del menu contestuale Windows. È possibile inoltre creare e gestire file vault direttamente dall'interfaccia Acronis Backup and Security 2010.

- Nella Modalità Intermedia, fare clic sulla scheda File Vault e usare le opzioni dall'area **Attività Veloci**. Una procedura guidata ti aiuterà a completare ogni attività.
- Per un approccio più diretto, passare l'interfaccia utente in Modalità Avanzata e fare clic su **Criptazione** dal menu a sinistra. Sulla scheda Criptazione File, è possibile vedere e gestire i file vault esistenti e il loro contenuto.

27.2.1. Crea Vault

Tenere a mente che un vault è di fatto solo un file con una estensione `.bvd`. Solo quando si apre il vault, appare un'unità disco virtuale in Risorse del computer ed è possibile archiviare in modo sicuro file al suo interno. Quando si crea un vault, è necessario specificare dove e con quale nome salvarlo sul computer. Inoltre è necessario specificare una password per proteggerne il contenuto. Solo utenti che conoscono la password possono aprire il vault e accedere a documenti e dati in esso archiviati.

Per creare un vault, eseguire questi passi:

1. Fare clic con il pulsante destro sul desktop o su una cartella del computer, puntare su **Acronis Backup and Security File Vault** e selezionare **Crea File Vault**. Apparirà la finestra seguente:

Crea File Vault

2. Specificare la posizione ed il nome del vault.
   - Cliccare su **Sfoglia**, selezionare la posizione del vault e salvare il file sotto il nome desiderato.
   - È sufficiente digitare il nome del vault nel campo corrispondente per crearlo in Documenti. Per aprire i Documenti, fare clic su start menu Start di Windows e poi **Documenti**.
   - Digitare il percorso completo del vault sul disco. Ad esempio, `C:\my_vault.bvd`.

3. Scegliere una lettera dal menu per il drive. Quando aprite il vault, un disco virtuale con la lettera selezionata apparirà su Risorse del Computer.
4. Digitare la password desiderata per il vault nei campi **Password** e **Conferma**. Qualsiasi persona che tenti di aprire il vault ed accedere ai suoi file, dovrà fornire la password.
5. Selezionare **Formattare drive** per formattare il disco virtuale assegnato al vault. È necessario formattare l'unità prima che si possa aggiungere file al vault.
6. Se desiderate cambiare la dimensione predefinita del vault (50 MB), digitare il valore desiderato nel campo **Dimensione del Vault**.
7. Cliccare su **Creare** se desiderate creare solo il vault nella destinazione selezionata. Per creare e mostrare il vault come un disco virtuale nelle Risorse del Computer, cliccare su **Creare & Aprire** .

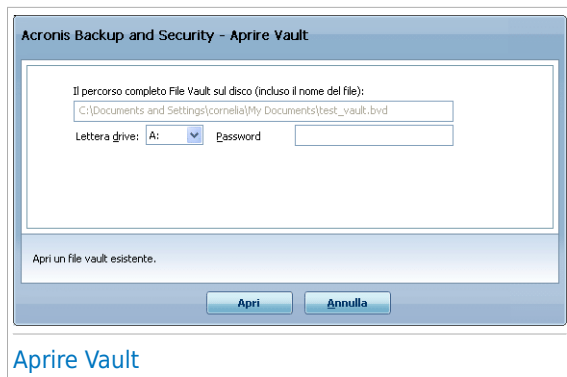
Acronis Backup and Security 2010 informerà immediatamente sul risultato dell'operazione. Se si verifica un errore, utilizzare il messaggio di errore per risolvere l'errore. Selezionare **OK** per chiudere la finestra.

Nota
Potrebbe essere conveniente salvare tutti i file vault nella stessa posizione. In questo modo, è possibili trovarli più velocemente.

27.2.2. Apri Vault

Per accedere e lavorare sui file immagazzinati in un vault, dovrete aprire il vault. Quando aprite un vault, apparirà un disco virtuale nelle Risorse del Computer. Il drive avrà la lettera di disco assegnata al vault.

Per aprire un vault, eseguire questi passi:

1. Individuare sul computer il `.bvd` file che rappresenta il vault che si vuole aprire.
2. Fare clic con il pulsante destro sul file, puntare su **Acronis Backup and Security File Vault** e selezionare **Apri**. Alternative più veloci sarebbero fare un doppio clic sul file, o fare clic con il pulsante di destra e selezionare **Apri**. Apparirà la finestra seguente:

Aprire Vault

3. Scegliere una lettera dal menu per il drive.
4. Digitare la password per il vault nel campo **Password**.
5. Cliccare **Aprire**.

Acronis Backup and Security 2010 informerà immediatamente sul risultato dell'operazione. Se si verifica un errore, utilizzare il messaggio di errore per risolvere l'errore. Selezionare **OK** per chiudere la finestra.

27.2.3. Blocca Vault

Quando abbiate finito di lavorare in un vault, dovrete bloccarlo per proteggere i vostri dati. Bloccando la vault, l'unità disco virtuale corrispondente sparisce da Risorse del computer. Di conseguenza l'accesso ai dati archiviati nel vault è completamente bloccato.

Per bloccare un vault, eseguire questi passi:

1. Aprire Documenti (fare clic su menu Start di Windows e poi **Risorse del computer**).
2. Identifica l'unità disco virtuale corrispondente al vault che si vuole chiudere. Cercare la lettera dell'unità assegnata al vault quando lo si è aperto.
3. Fare clic con il pulsante destro sull'unità disco virtuale corrispondente, puntare su **Acronis Backup and Security File Vault** e fare clic su **Blocca**.

E' anche possibile fare clic con il tasto destro sul file .bvd che rappresenta il vault, puntare su **Acronis Backup and Security File Vault** e fare clic su **Blocca**.

Acronis Backup and Security 2010 informerà immediatamente sul risultato dell'operazione. Se si verifica un errore, utilizzare il messaggio di errore per risolvere l'errore. Selezionare **OK** per chiudere la finestra.

Nota

Se sono aperti diversi vault, si consiglia di usare l'interfaccia Modalità Avanzata Acronis Backup and Security 2010. Se si fa clic sulla scheda **Criptazione**, Criptazione File, è possibile vedere una tabella che fornisce informazioni sui vault esistenti. Queste informazioni includono l'eventuale apertura del vault e, in tal caso, la lettera assegnata all'unità.

27.2.4. Aggiungi a file vault

Prima che sia possibile aggiungere file o cartelle ad un vault, è necessario aprire il vault. Una volta che il vault è aperto, è possibile archiviare facilmente file o cartelle all'interno per utilizzare il menu contestuale. Fare clic con il pulsante destro sul file o cartella che si vuole copiare nel vault, puntare su **Acronis Backup and Security File Vault** e fare clic su **Aggiungi a file vault**.

- Se solo un vault è aperto, il file o la cartella è copiata direttamente a quel vault.
- Se diversi vault sono aperti, verrà chiesto di scegliere il vault in cui copiare l'elemento. Selezionare dal menu la lettera dell'unità corrispondente al vault desiderato e fare clic su **OK** per copiare l'elemento.

È inoltre possibile utilizzare l'unità disco virtuale corrispondente al vault. Attenersi alla seguente procedura:

1. Aprire Documenti (fare clic su start menu Start di Windows e poi **Risorse del computer**).
2. Inserire l'unità disco virtuale corrispondente al vault. Cercare la lettera dell'unità assegnata al vault quando lo si è aperto.
3. Copia e incolla e trascina file e cartelle direttamente a questa unità disco virtuale.

27.2.5. Rimuovi dal file vault

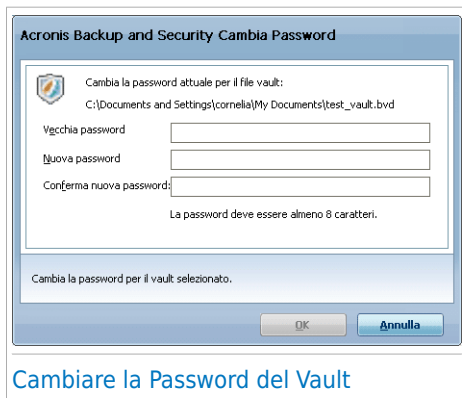
Per rimuovere i file o cartelle da un vault, il vault deve essere aperto. Per rimuovere file o cartelle da un vault, eseguire questi passi:

1. Aprire Documenti (fare clic su start menu Start di Windows e poi **Risorse del computer**).
2. Inserire l'unità disco virtuale corrispondente al vault. Cercare la lettera dell'unità assegnata al vault quando lo si è aperto.
3. Rimuove file o cartelle come si fa normalmente in Windows (ad esempio, fare clic con il pulsante destro su un file che si vuole eliminare e selezionare **Elimina**).

27.2.6. Cambiare la Password del Vault

La password protegge il contenuto di un vault da accessi non autorizzati. Solo utenti che conoscono la password possono aprire il vault e accedere a documenti e dati in esso archiviati.

Il vault deve essere bloccato prima che si possa cambiare la sua password. er cambiare la password di un vault, eseguire questi passi:

1. Individuare sul computer il `.bvd` file che rappresenta il vault.
2. Fare clic con il pulsante destro sul file, puntare su **Acronis Backup and Security File Vault** e selezionare **Modifica Password Vault**. Apparirà la finestra seguente:

Cambiare la Password del Vault

3. Digitare la password corrente del vault nel campo **Vecchia Password**.
4. Digitare la nuova password del vault nei campi **Nuova password** e **Conferma Nuova Password**.

Nota

La password deve essere composta da almeno 8 caratteri. Per avere una password forte, utilizzare una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, $ o @).

5. Cliccare su **OK** per cambiare la password.

Acronis Backup and Security 2010 informerà immediatamente sul risultato dell'operazione. Se si verifica un errore, utilizzare il messaggio di errore per risolvere l'errore. Selezionare **OK** per chiudere la finestra.

28. Integrazione nei Web Browser

Acronis Backup and Security 2010 vi protegge da tentativi di phishing mentre navigate in Internet. Esamina i siti web visitati e vi allerta se ci sono minacce di phishing. Può essere configurata una White List di siti web che non vogliate vengano esaminati da Acronis Backup and Security 2010.

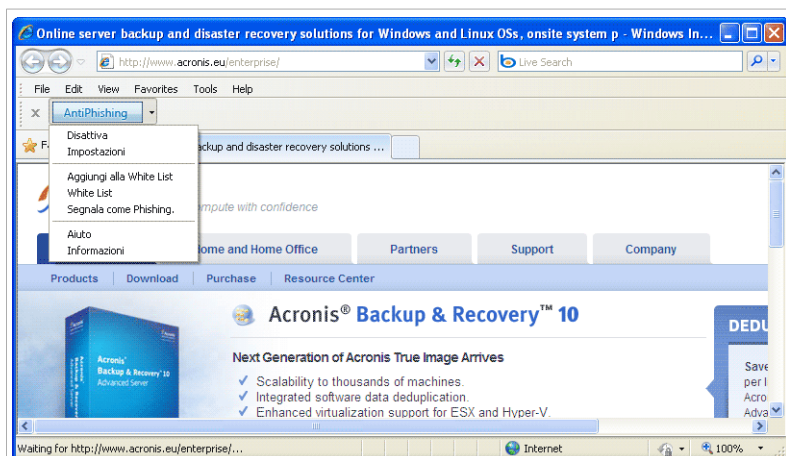
Acronis Backup and Security 2010 si integra direttamente attraverso una barra degli strumenti intuitiva e di facile uso nei seguenti web browser:

- Internet Explorer
- Mozilla Firefox

Potete gestire facilmente ed efficacemente la protezione antiphishing e la White List utilizzando la barra degli strumenti Antiphishing Acronis integrata nei web browser citati sopra.

La barra degli strumenti antiphishing si trova nella parte superiore del browser. Cliccare sopra per aprire il menu della barra degli strumenti.

Nota

Se non potete visualizzare la barra degli strumenti, aprire il menu **Visualizzare**, puntare su **Barre degli strumenti** e selezionare **Barra degli strumenti Acronis**.

Barra degli Strumenti Antiphishing

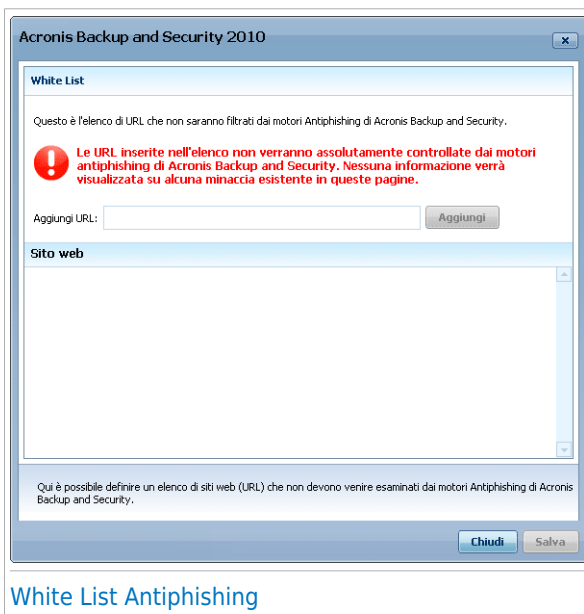
Nella barra degli strumenti sono disponibili i seguenti comandi:

- **Attivare / Disattivare** - attiva / disattiva la protezione Antiphishing di Acronis Backup and Security 2010 nel browser web attuale.

- **Impostazioni** - apre una finestra dove potete specificare le impostazioni della barra degli strumenti Antiphishing. Sono disponibili le seguenti opzioni:
  - **La protezione Web Antiphishing in tempo reale** - individua e avverte in tempo reale se un sito web è oggetto di phishing (impostato per rubare informazioni personali). Questa opzione controlla la protezione antiphishing Acronis Backup and Security 2010 solo nel browser web attuale.
  - **Chiedere prima di aggiungere alla White List** - vi viene chiesto prima di aggiungere un sito web alla White List.
- **Aggiungere alla White List** - aggiunge il sito web corrente alla White List.

Nota

Aggiungere un sito alla White List significa che Acronis Backup and Security 2010 non esaminerà più il sito per tentativi di phishing. Vi consigliamo di aggiungere alla White List solo siti di cui vi fidate pienamente.

- **White List** - apre la White List.

White List Antiphishing

Potete vedere la lista di tutti i siti web che non vengono controllati dai motori di antiphishing Acronis Backup and Security 2010. Se si vuole rimuovere un sito dalla White List in modo che sia notificata qualsiasi minaccia di phishing su quella pagina, fare clic sul pulsante **Rimuovi** a fianco.

Potete aggiungere i siti di cui vi fidate pienamente alla White List, in modo che non verranno più esaminati dai motori antiphishing. Per aggiungere un sito alla White List, inserire il suo indirizzo nel campo corrispondente e quindi cliccare **Aggiungere**.

- **Segnala come phishing** - informa il Laboratorio Acronis che si considera il relativo sito web come sito usato per phishing. Segnalando siti web di phishing si aiuta a proteggere altri da furti di identità.
- **Aiuto** - apre la documentazione elettronica.
- **Informazioni** - apre una finestra nella quale è possibile visualizzare delle informazioni su Acronis Backup and Security 2010 e cercare aiuto nel caso in cui accada qualcosa di inaspettato.

29. Integrazione in Programmi Instant Messenger

Acronis Backup and Security 2010 offre delle capacità di criptazione per proteggere i vostri documenti confidenziali e le vostre conversazioni attraverso Yahoo Messenger e MSN Messenger.

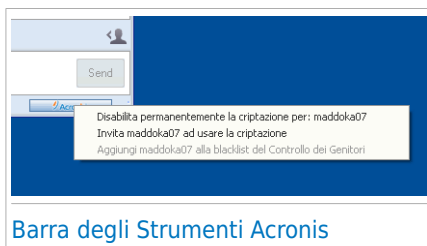
Di default, Acronis Backup and Security 2010 esegue la criptazione di tutte le vostre sessioni chat, purché:

- Il tuo partner di chat abbia un prodotto di Acronis installata che supporti la Criptazione Chat, e la Criptazione Chat sia abilitata per l'applicazione usata per chattare.
- Tu ed il tuo partner di chat usate entrambi Yahoo Messenger o Windows Live (MSN) Messenger.

Importante

Acronis Backup and Security 2010 non eseguirà la criptazione di una conversazione se uno dei partner utilizza un'applicazione chat su web, come Meebo, o altra applicazione chat che supporti Yahoo Messenger o MSN.

Potete configurare facilmente la criptazione dell'instant messaging utilizzando la barra degli strumenti di Acronis nella finestra di chat. La barra degli strumenti dovrebbe essere posizionata in basso a destra della finestra chat. Cercare il logo Acronis per trovarla.

Barra degli Strumenti Acronis

Nota

La barra degli strumenti indicate che una conversazione è criptata mostrando una piccola chiave vicino al logotipo Acronis.

Facendo clic sulla barra degli strumenti di Acronis appaiono le seguenti opzioni:

- **Disabilita criptazione per sempre per `contatto`.**
- **Invita `contatto` ad usare la criptazione.** Per criptare le conversazioni, il contatto deve installare Acronis Backup and Security 2010 e utilizzare un programma IM compatibile.
- **Aggiungi `contatto` alla blacklist Controllo genitori.** Se si aggiunge un contatto alla blacklist Controllo genitori e il Controllo genitori è abilitato, non si vedranno più i messaggi chat inviati da tale contatto. Per rimuovere il contatto dalla blacklist, fare clic sulla barra degli strumenti e selezionare **Rimuovi `contatto` dalla blacklist Controllo genitori**.

30. Integrazione nei client di posta

Acronis Backup and Security 2010 include un modulo Antispam. Antispam verifica i messaggi e-mail che si ricevono e identifica quelli che sono spam. I messaggi spam rilevati da Acronis Backup and Security 2010 sono marcati con il prefisso `[SPAM]` nell'oggetto.

Nota

È fornita una protezione antispam per tutti i client di posta POP3/SMTP.

Acronis Backup and Security 2010 si integra direttamente attraverso una barra degli strumenti intuitiva e di facile uso nei seguenti client di posta:

- Microsoft Outlook
- Outlook Express
- Windows Mail
- Mozilla Thunderbird

Acronis Backup and Security 2010 sposta automaticamente messaggi spam ad una cartella specifica, come segue:

- In Microsoft Outlook, i messaggi spam sono spostati nella cartella **Spam**, situata nella cartella **Posta eliminata**. La cartella **Spam** è creata durante l'installazione di Acronis Backup and Security 2010.
- In Outlook Express e Windows Mail, i messaggi spam sono spostati direttamente nella cartella **Posta eliminata**.
- In Mozilla Thunderbird, i messaggi spam sono spostati nella cartella **Spam**, situata nella cartella **Cestino**. La cartella **Spam** è creata durante l'installazione di Acronis Backup and Security 2010.

Se si utilizza un altro client per la posta, è necessario creare una regola per spostare i messaggi e-mail segnati come `[SPAM]` da Acronis Backup and Security 2010 in una cartella personalizzata di quarantena.

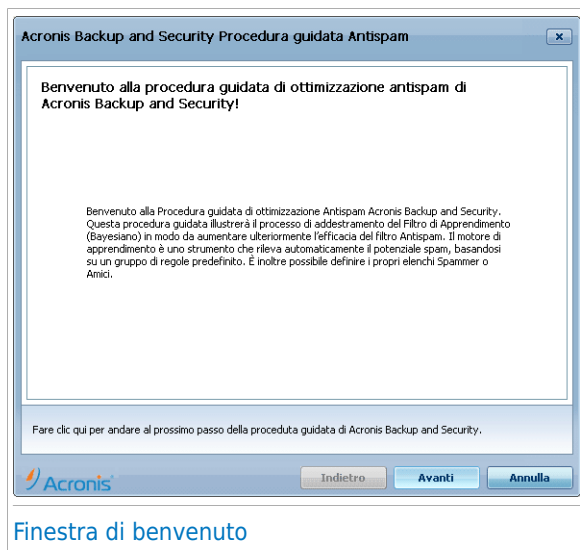
30.1. Assistente per la Configurazione Antispam

La prima volta che lanciate il vostro client di posta con Acronis Backup and Security 2010 installato, apparirà l'assistente per aiutarvi a configurare l' Elenco Amici, l' Elenco Spammers e per istruire il Filtro Bayesiano in modo da aumentare l'efficienza dei filtri Antispam.

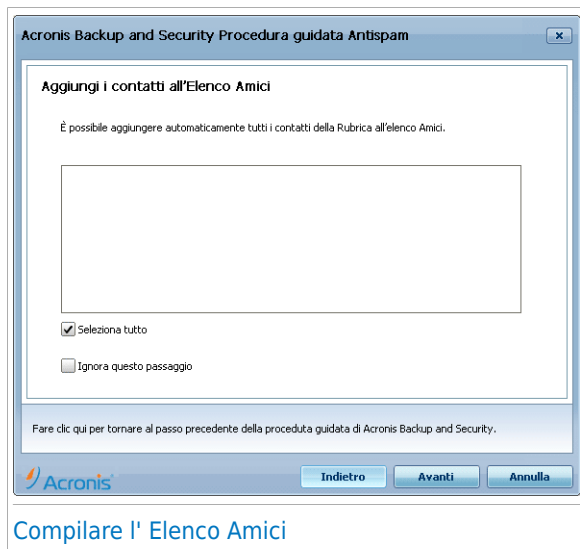
Nota

La procedura guidata può essere lanciata quando si vuole facendo clic sul pulsante **Procedura guidata** nella barra degli strumenti Antispam.

30.1.1. Passo 1/6 - Finestra di Benvenuto

Finestra di benvenuto

Selezionare **Avanti**.

30.1.2. Passo 2/6 - Compilare l' Elenco Amici

Compilare l' Elenco Amici

Da qui è possibile vedere tutti gli indirizzi della vostra **Rubrica**. Selezionare quelli che si desidera aggiungere al vostro **elenco Amici** (suggeriamo di selezionarli tutti). Si riceveranno tutti i messaggi e-mail provenienti da questi indirizzi, indipendentemente dal loro contenuto.

Per aggiungere tutti i vostri contatti all'elenco degli Amici, selezionare **Selezionare tutti**.

Se si desidera ignorare questo passaggio di configurazione, selezionare **Ignora questo passaggio**. Selezionare **Successivo** per continuare.

30.1.3. Passo 3/6 - Cancellare il Database Bayesiano

Cancellare il Database Bayesiano

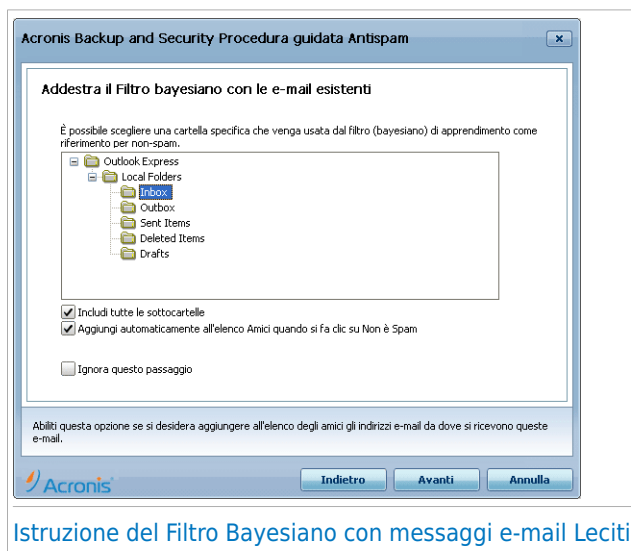
Nel tempo, si potrà notare che il vostro Filtro Antispam comincia ad essere meno efficace. Il motivo potrebbe essere quello di un addestramento improprio (ovvero nel caso in cui si sia erroneamente marcato un certo numero di messaggi legittimi come Spam e viceversa). Se il vostro filtro risulta essere molto in accurato, potrebbe essere necessario pulire il database del filtro e addestrare nuovamente il filtro seguendo le fasi successive di questa guida.

Selezionare **Pulisci il database del filtro antispam** se si desidera impostare nuovamente il database Bayesiano.

E' possibile salvare il database Bayesiano su un file in modo da poterlo utilizzarecon un altro prodotto Acronis Backup and Security 2010 o dopo aver reinstallato Acronis Backup and Security 2010. Per salvare il database Bayesiano, fare clic sul pulsante **Salva Bayes** e salvare nella posizione desiderata. Il file avrà estensione `.dat`.

Per caricare un database Bayesiano precedentemente salvato, fare clic sul pulsante **Carica Bayes** e aprire il file corrispondente.

Se si desidera ignorare questo passaggio di configurazione, selezionare **Ignora questo passaggio**. Selezionare **Successivo** per continuare.

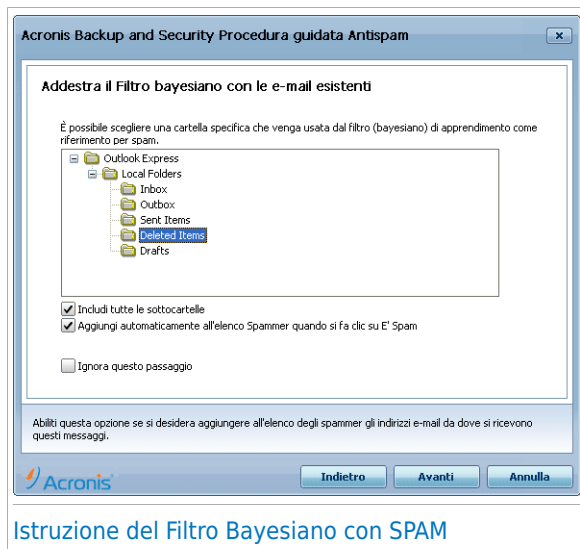
30.1.4. Passo 4/6 - Istruzione del Filtro Bayesiano con messaggi e-mail Leciti

Istruzione del Filtro Bayesiano con messaggi e-mail Leciti

Selezionare una cartella che contenga messaggi e-mail leciti. Questi messaggi verranno utilizzati per addestrare il filtro Antispam.

Ci sono due opzioni avanzate sotto la lista delle directory:

- **Includi sottocartelle** - per includere le sottocartelle nella selezione.
- **Aggiungi automaticamente all'elenco Amici** - per aggiungere i mittenti all'elenco degli Amici.

Se si desidera ignorare questo passaggio di configurazione, selezionare **Ignora questo passaggio**. Selezionare **Successivo** per continuare.

30.1.5. Passo 5/6 - Istruzione del Filtro Bayesiano con SPAM

Istruzione del Filtro Bayesiano con SPAM

Selezionare una cartella che contenga messaggi e-mail Spam. Questi messaggi verranno utilizzati per addestrare il filtro Antispam.

Importante

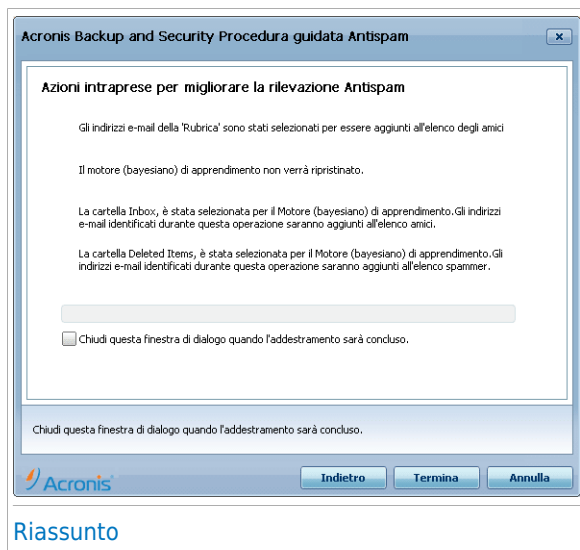
Assicurarsi che la cartella scelta non contenga assolutamente e-mail lecite, altrimenti la prestazione antispam verrà notevolmente ridotta.

Ci sono due opzioni avanzate sotto la lista delle directory:

- **Includi sottocartelle** - per includere le sottocartelle nella selezione.
- **Aggiungi automaticamente all'elenco Spammer** - per aggiungere i mittenti all'elenco degli Spammer. I messaggi e-mail da questi mittenti verranno sempre identificati come SPAM e trattati di conseguenza.

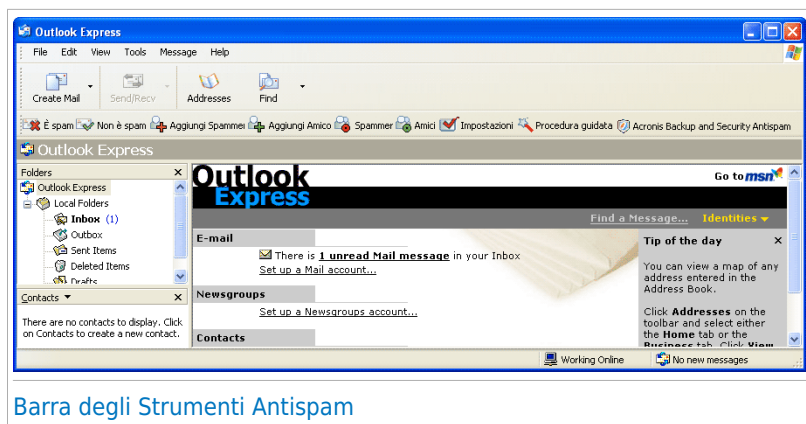
Se si desidera ignorare questo passaggio di configurazione, selezionare **Ignora questo passaggio**. Selezionare **Successivo** per continuare.

30.1.6. Passo 6/6 – Sommario

Riassunto

In questa finestra si potranno osservare tutte le impostazioni della guida alla configurazione. Si potrà eseguire qualsiasi modifica ritornando la passo precedente (selezionare **Indietro**).

Se tu non vuoi apportare modifiche, clicca **Fine** per terminare la configurazione.

30.2. Barra degli Strumenti Antispam

Nella parte superiore della finestra del client di posta è possibile vedere la Barra degli Strumenti Antispam. La barra degli strumenti Antispam aiuta a gestire la protezione antispam direttamente dal client di posta. È possibile correggere facilmente Acronis Backup and Security 2010 se segnala un messaggio legittimo come SPAM.

Barra degli Strumenti Antispam

Qui di seguito la spiegazione di ogni pulsante:

- **E' Spam** - invia un messaggio al modulo Bayesiano indicando che la mail selezionata è spam. La mail sarà marcata come SPAM e verrà spostata nella cartella **Spam**.

  I futuri messaggi con caratteristiche uguali verranno marcati come Spam.

Nota
E' possibile selezionare uno o più messaggi e-mail come si desidera.

- **Non è Spam** - invia un messaggio al modulo Bayesiano indicando che la mail selezionata non è spam e Acronis Backup and Security 2010 non avrebbe dovuto classificarla come tale. L'e-mail verrà spostata dalla cartella **Spam** alla directory **Inbox**.

  I futuri messaggi con caratteristiche uguali non verranno più marcati come Spam.

Nota
E' possibile selezionare uno o più messaggi e-mail come si desidera.

Importante
Il pulsante **Non è spam** si attiva quando si seleziona un messaggio marcato come SPAM da Acronis Backup and Security 2010 (normalmente questi messaggi sono situati nella cartella **Spam**).

- **Aggiungi Spammer** - aggiunge il mittente dell'e-mail selezionata all'elenco degli Spammer.

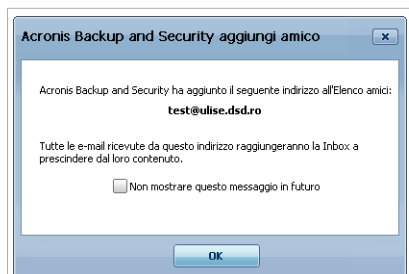
Aggiungi Spammer

Selezionare **Non mostrare questo messaggio in futuro** se non si desidera la richiesta di conferma quando si aggiunge un indirizzo spammer all'elenco.

Selezionare **OK** per chiudere la finestra.

Le future e-mail provenienti da questo indirizzo verranno marcate come Spam.

Nota
E' possibile selezionare uno o più mittenti e-mail come si desidera.

- **Aggiungi Amici** - aggiunge il mittente dell'e-mail selezionata all'elenco degli Amici.

Aggiungi Amico

Selezionare **Non mostrare questo messaggio in futuro** se non si desidera la richiesta di conferma quando si aggiunge un indirizzo di amici all'elenco.

Selezionare **OK** per chiudere la finestra.

Si riceveranno sempre email provenienti da questo indirizzo, indipendentemente dal contenuto del messaggio.

Nota
E' possibile selezionare uno o più mittenti e-mail come si desidera.

- **Spammers** - apre l'**Elenco Spammers**, il quale contiene tutti gli indirizzi mail dai quali non volete ricevere messaggi, indipendentemente dal loro contenuto.

Nota
Qualsiasi mail in arrivo da un indirizzo contenuto nell'**Elenco Spammer** verrà automaticamente marcato come Spam, senza alcun ulteriore processo.

Elenco Spammers

Qui potrete aggiungere o rimuovere elementi dall'**Elenco Spammer**.

Se si desidera aggiungere un indirizzo email, spuntare l' opzione **Indirizzo Email**, digitare l'indirizzo e selezionare il pulsante ▷. L'indirizzo apparirà nell'**Elenco Spammers**.

Importante
Sintassi: name@domain.com.

Se desiderate aggiungere un dominio, selezionare il campo **Dominio**, introdurre il nome e premere il pulsante ▷. Il dominio apparirà nell'**Elenco Spammers**.

Importante
Sintassi:

- @domain.com, *domain.com e domain.com - tutte le mail provenienti da domain.com verranno marcate come Spam;
- *domain* - tutte le mail provenienti da domain (indipendentemente dai suffissi del dominio) verranno marcate come Spam;
- *com - tutte le mail con il suffisso di dominio com verranno marcate come Spam.

Avvertimento

Non aggiungere domini di servizi e-mail legittimi (ad esempio Yahoo, Gmail, Hotmail o altri) all'elenco Spammer. In caso contrario gli indirizzi e-mail ricevuti dagli utenti registrati di tali servizi verranno identificati come spam. Se ad esempio si aggiunge `yahoo.com` all'elenco Spammer, tutti i messaggi e-mail provenienti da indirizzi `yahoo.com` saranno contrassegnati come `[spam]`.

Per importare gli indirizzi e-mail da **Rubrica di Windows** / **Cartelle di Outlook Express** a **Microsoft Outlook** / **Outlook Express** / **Windows Mail** selezionare l'opzione appropriata dal menu a tendina **Importa indirizzi e-mail da**.

Per **Microsoft Outlook Express / Windows Mail** apparirà una nuova finestra dove potete selezionare la cartella che contiene gli indirizzi mail che volete aggiungere all'**Elenco Spammer**. Sceglieteli e cliccate su **Seleziona**.

In entrambi i casi gli indirizzi e-mail appariranno nella lista di importazione. Selezionare quelli desiderati e fare clic su ⊠ per aggiungerli all'**Elenco Spammer**. Facendo clic su ⊠ tutti gli indirizzi verranno aggiunti all'elenco.

Per rimuovere un elemento dall'elenco, selezionarlo e fare clic su **Rimuovi**. Per eliminare tutti gli elementi dall'elenco fare clic su **Pulisci elenco** e quindi su **Sì** per confermare.

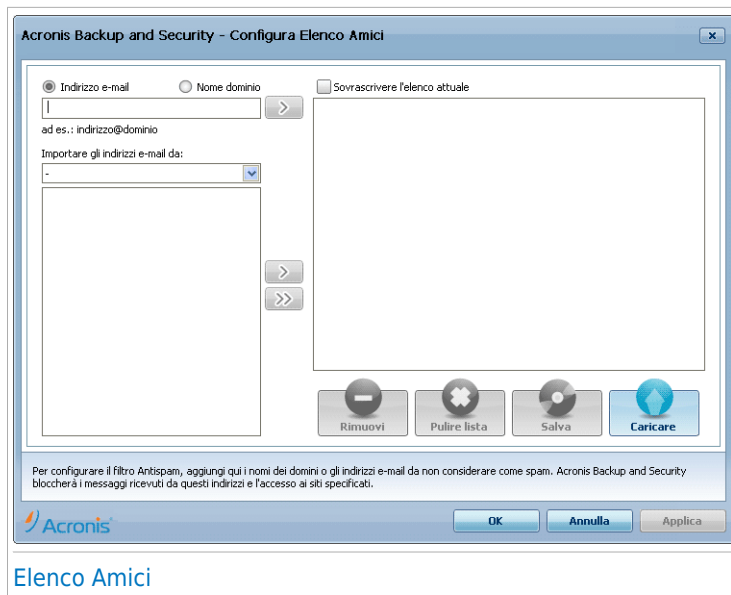
E' possibile salvare l'elenco Spammer in un file in modo da poterlo riutilizzare su un altro computer o dopo aver reinstallato il prodotto. Per salvare l'elenco Spammer, fare clic sul pulsante **Salva** e salvare nella posizione desiderata. Il file avrà estensione `.bwl`.

Per caricare un elenco Spammer precedentemente salvato, fare clic sul pulsante **Carica** e aprire il corrispondente file `.bwl`. Per ripristinare il contenuto dell'elenco esistente quando si carica un elenco precedentemente salvato, selezionare **Sovrascrivi l'elenco attuale**.

Selezionare **Applica** e **OK** tper salvare & chiudere **l'Elenco Spammer**.

- **Amici** - apre l'**Elenco Amici** che contiene tutti gli indirizzi mail dai quali volete ricevere sempre i messaggi, indipendentemente dal loro contenuto.

Nota

Qualsiasi mail in arrivo da un indirizzo contenuto nella lista **Elenco Amici**, sarà automaticamente consegnato alla vostra Inbox senza alcun ulteriore processo.

Elenco Amici

Qui potrete aggiungere o rimuovere elementi dall'**Elenco Amici**.

Se si desidera aggiungere un indirizzo email, spuntare il campo **Indirizzo Email**, digitare l'indirizzo e selezionare il pulsante ⊠. L'indirizzo apparirà nell'**Elenco Spammers**.

Importante

Sintassi: name@domain.com.

Se desiderate aggiungere un dominio, selezionare l' opzione **Dominio**, digitare il nome e premere il pulsante ⊠. Il dominio apparirà nell'**Elenco Amici**.

Importante

Sintassi:

- @domain.com, *domain.com e domain.com - tutte le mail provenienti da domain.com raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;
- *domain* - tutte le mail provenienti da domain (non importa il suffisso del dominio) raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;
- *com - tutte le mail con il suffisso di dominio com raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;

Per importare gli indirizzi e-mail da **Rubrica di Windows** / **Cartelle di Outlook Express** a **Microsoft Outlook** / **Outlook Express** / **Windows Mail** selezionare l'opzione appropriata dal menu a tendina **Importa indirizzi e-mail da**.

Per **Microsoft Outlook Express** apparirà una nuova finestra dove potrete selezionare la cartella che contiene gli indirizzi mail che vorrete aggiungere all'**Elenco Amici**. Sceglierli e cliccare su **Seleziona**.

In entrambi i casi gli indirizzi e-mail appariranno nella lista di importazione. Selezionare quelli desiderati e fare clic su per aggiungerli all'**Elenco Amici**. Facendo clic su tutti gli indirizzi verranno aggiunti all'elenco.

Per rimuovere un elemento dall'elenco, selezionarlo e fare clic su **Rimuovi**. Per eliminare tutti gli elementi dall'elenco fare clic su **Pulisci elenco** e quindi su **Sì** per confermare.

E' possibile salvare l'elenco Amici in un file in modo da poterlo riutilizzare su un altro computer o dopo aver reinstallato il prodotto. Per salvare l'elenco Amici, fare clic sul pulsante **Salva** e salvare nella posizione desiderata. Il file avrà estensione `.bwl`.

Per caricare un elenco Amici precedentemente salvato, fare clic sul pulsante **Carica** e aprire il corrispondente file `.bwl`. Per ripristinare il contenuto dell'elenco esistente quando si carica un elenco precedentemente salvato, selezionare **Sovrascrivi l'elenco attuale**.

Nota

Raccomandiamo di aggiungere i nomi dei vostri amici e gli indirizzi e-mail all'**elenco Amici**. Acronis Backup and Security 2010 non blocca i messaggi di coloro che sono nell'elenco; aggiungere amici aiuta a garantire che i messaggi leciti vengano recapitati.

Selezionare **Applica** e **OK** per salvare & chiudere **l'Elenco Amici**.

- **Impostazioni** - apre la finestra **Impostazioni** dove potete specificare alcune opzioni per il modulo **Antispam**.

Impostazioni

Sono disponibili le seguenti opzioni:

- **Sposta il messaggio in Elementi Cancellati** - sposta i messaggi spam nella cartella **Elementi Cancellati** (solo per Microsoft Outlook Express / Windows Mail);
- **Marcare il messaggio come letto** - per marcare tutti i messaggi Spam come letti così da non essere disturbati quando arrivano nuovi messaggi Spam.

Se il vostro filtro antispam è molto impreciso, può rendersi necessario pulire il database del filtro e addestrare nuovamente il Filtro Bayesiano. Selezionare **Pulisci il database dell'antispam** se si desidera impostare nuovamente il database Bayesiano.

E' possibile salvare il database Bayesiano su un file in modo da poterlo utilizzarecon un altro prodotto Acronis Backup and Security 2010 o dopo aver reinstallato Acronis Backup and Security 2010. Per salvare il database Bayesiano, fare clic sul pulsante **Salva Bayes** e salvare nella posizione desiderata. Il file avrà estensione `.dat`.

Per caricare un database Bayesiano precedentemente salvato, fare clic sul pulsante **Carica Bayes** e aprire il file corrispondente.

Selezionare la tabella **Avvisi** se desiderate accedere alla sezione dove è possibile disattivare la comparsa della finestra di conferma per le opzioni **Aggiungere spammer** ed **Aggiungere amico**.

Nota

Nella finestra **Avvisi** potete anche abilitare / disabilitare la comparsa dell'avviso **Seleziona un messaggio e-mail**. Questo avviso compare quando selezionate un gruppo invece di un messaggio e-mail.

- **Procedura guidata** - apre la Procedura guidata configurazione antispam, ce aiuterà ad addestrare il filtro bayesiano per aumentare ulteriormente l'efficacia del filtraggio Acronis Backup and Security 2010 Antispam. Inoltre è possibile aggiungere indirizzi dall'Agenda all'elenco Amici / Spammer.
- **Acronis Backup and Security Antispam** - apre l'interfaccia Acronis Backup and Security 2010.

Come fare

31. Scansione di file e cartelle

La scansione è facile e flessibile con Acronis Backup and Security 2010. Ci sono 4 modi per impostare Acronis a scansionare file e cartelle per virus e altro malware:

- Utilizzando il Menu Contestuale Windows
- Utilizzando attività di scansione
- Utilizzando la scansione manuale di Acronis
- Utilizzando la barra attività di scansione

Una volta avviata la scansione, apparirà la procedura guidata di Scansione che illustra il processo. Per ulteriori informazioni sulla procedura guidata, far riferimento a *«Procedura guidata scansione antivirus»* (p. 46).

31.1. Utilizzando il Menu Contestuale Windows

Si tratta del modo più semplice e consigliato per scansionare un file o una cartella sul computer. Fare clic con il pulsante destro del mouse sull'oggetto che si desidera scansionare e selezionare dal menu **Scansiona con Acronis Backup and Security**. Seguire le istruzioni della procedura guidata Scansione Antivirus per eseguire la scansione.

Tipiche situazioni in cui si userebbe questo metodo includono:

- Si sospetta che un file o una cartella specifica sia infetta.
- Ogni volta che si scarica un file di Internet che potrebebro essere pericolosi.
- Scansionare una condivisione di rete prima di copiare i file sul computer.

31.2. Utilizzando attività di scansione

Se si desidera scansionare il computer o cartelle specifiche regolarmente, si consiglia di considerare l'utilizzo delle attività di scansione. Le attività di scansione istruisce Acronis Backup and Security 2010 in merito a quali ubicazioni scansionare, e quali opzioni di scansione e azioni applicare. Inoltre, è possibile programmare tali azioni per eseguirle regolarmente o in momenti specifici.

Per scansionare il computer utilizzando attività di scansione, è necessario aprire l'interfaccia Acronis Backup and Security 2010 ed eseguire le attività di scansione desiderate. A seconda della modalità di visualizzazione dell'interfaccia, si devono eseguire differenti passi per eseguire attività di scansione.

Esecuzione attività di scansione nella modalità inesperto

Nella modalità inesperto, è possibile eseguire solo una scansione di tutto il computer facendo clic su **Scansiona ora**. Seguire le istruzioni della procedura guidata Scansione Antivirus per eseguire la scansione.

Esecuzione attività di scansione nella modalità intermedia

Nella Modalità Intermedia, è possibile eseguire diverse attività di scansione pre-configurate. È possibile inoltre configurare ed eseguire scansioni personalizzate per scansionare ubicazioni specifiche sul computer usando opzioni di scansione personalizzate. Eseguire questi passi per eseguire una attività di scansione nella Modalità Intermedia:

1. Fare clic sulla scheda **Sicurezza**.
2. Sulla sinistra dell'area Attività veloci, fare clic su **Scansione del sistema** per avviare una scansione standard di tutto il computer. Per eseguire una attività di scansione differente, fare clic sulla freccia sul fondo e selezionare l'attività di scansione desiderata. Per configurare ed eseguire una scansione personalizzata, fare clic su **Scansione Personalizzata**. Queste sono le attività di scansione disponibili:

Funzione di Scansione	Descrizione
Scansione sistema	Esamina l'intero sistema, esclusi gli archivi. Nella configurazione di default la scansione ricerca tutti i tipi di malware ad eccezione dei rootkit.
Scansione del Sistema approfondita	Esamina l'intero sistema. Nella configurazione predefinita, esegue la scansione per tutti i tipi di malware che minacciano la sicurezza del vostro sistema, come virus, spyware, adware, rootkits ed altri.
Scansione Documenti	Utilizzare questa funzione per esaminare delle cartelle importanti dell'utente corrente: `My Documents`, `Desktop` e `StartUp`. Questo garantirà la sicurezza dei vostri documenti, uno spazio di lavoro sicuro ed applicazioni pulite al avvio.
Personalizzare Scansione	Questa opzione permette di configurare ed eseguire un'attività di scansione personalizzata, permettendo di specificare cosa esaminare e quali opzioni generali di scansione utilizzare. È possibile salvare le attività di scansione personalizzate in modo da poterle utilizzare di nuovo in Modalità Intermedia o Avanzata.

3. Seguire le istruzioni della procedura guidata Scansione Antivirus per eseguire la scansione. Se si sceglie di eseguire una scansione personalizzata, è necessario completare l'assistente Scansione Personalizzata.

Esecuzione attività di scansione in Modalità Avanzata

In Modalità avanzata è possibile eseguire tutte le attività di scansione pre-configurate e modificare le opzioni di scansione. Inoltre è possibile creare attività di scansione personalizzate se si desidera scansionare parti specifiche del computer. Eseguire questi passi per eseguire un'attività di scansione in Modalità Avanzata:

1. Clicca su **Antivirus** dal menù a sinistra.
2. Fare clic sulla scheda **Scansione Virus**. Qui è possibile trovare un numero di attività di scansione di default ed è possibile creare le proprie attività di scansione. Queste sono le attività di scansione predefinite che si possono utilizzare:

Funzione di Default	Descrizione
Scansione del Sistema approfondita	Esamina l'intero sistema. Nella configurazione predefinita, esegue la scansione per tutti i tipi di malware che minacciano la sicurezza del vostro sistema, come virus, spyware, adware, rootkits ed altri.
Scansione sistema	Esamina l'intero sistema, esclusi gli archivi. Nella configurazione di default la scansione ricerca tutti i tipi di malware ad eccezione dei rootkit.
Scansione Veloce del Sistema	Scansiona le cartelle `Windows` e `Program Files`. Nella configurazione predefinita, esamina per cercare tutti i tipi di malware, esclusi i rootkit, ma non esamina la memoria, il registro nè i cookies.
Documenti	Utilizzare questa funzione per esaminare delle cartelle importanti dell'utente corrente: `My Documents`, `Desktop` e `StartUp`. Questo garantirà la sicurezza dei vostri documenti, uno spazio di lavoro sicuro ed applicazioni pulite al avvio.

3. Fare un doppio clic sull'attività di scansione che si desidera eseguire.
4. Seguire le istruzioni della procedura guidata Scansione Antivirus per eseguire la scansione.

31.3. Utilizzando la scansione manuale Acronis

La scansione Manuale Acronis consente di scansionare cartelle o partizioni di disco rigido specifiche senza dover creare una attività di scansione. Questa funzionalità è stata progettata per essere utilizzata quando Windows è in Modalità provvisoria. Se il sistema è infettato con un virus resistente, si può provare a rimuovere il virus avviando Windows nella Modalità provvisoria e eseguendo la scansione di ogni partizione di disco rigido usando Acronis Manual Scan.

Per scansionare il computer utilizzando la Scansione Manuale di Acronis, eseguire i seguenti passi:

1. Sul menu start Start di Windows, seguire il percorso **Start** → **Programmi** → **Acronis** → **Acronis Backup and Security 2010** → **Scansione manuale Acronis**. Apparirà una nuova finestra.
2. Fare clic su **Aggiungi Cartella** per selezionare l'obbiettivo della scansione. Apparirà una nuova finestra.
3. Selezionare il target di scansione:
   - Per eseguire una scansione del desktop, selezionare **Desktop**.
   - Per scansionare un'intera partizione di un disco rigido, selezionarla da Risorse del computer.
   - Per scansionare una cartella specifica, cercare tale cartella e selezionarla.
4. Selezionare **OK**.
5. Fare clic su **Continua** per avviare la scansione.
6. Seguire le istruzioni della procedura guidata Scansione Antivirus per eseguire la scansione.

Cos'è la Modalità provvisoria?
La modalità provvisoria è un modo speciale di avviare Windows, usata principalmente per risolvere problemi che influenzano il normale funzionamento di Windows. Tali problemi vanno da driver in conflitto a virus che impediscono a Windows di avviarsi normalmente. Nella Modalità provvisoria, Windows carica solo una parte minima di componenti del sistema operativo e dei driver fondamentali. Solo alcune applicazioni funzionano nella Modalità provvisoria. Ecco perché la maggior parte del virus sono inattivi quando si utilizza Windows nella Modalità provvisoria e perché possono essere facilmente rimossi.
Per avviare Windows nella Modalità provvisoria, riavviare il computer e premere il tasto F8 fino a quando appare il Menu opzioni avanzate di Windows. È possibile scegliere tra varie opzioni di Windows nella Modalità provvisoria. Si può selezionare **Modalità provvisoria con Networking** per abilitare l'accesso a Internet.

Nota

Per ulteriori informazioni sulla Modalità provvisoria, fare clic su Guida e Supporto tecnico di Windows (nel menu Start, fare clic su **Guida e Supporto tecnico**). È inoltre possibile trovare informazioni utili cercando su Internet.

31.4. Utilizzo della Barra delle Attività di Scansione

La **Barra delle attività di scansione** è una visualizzazione grafica dell'attività di scansione sul vostro sistema. Questa piccola finestra è disponibile per default solo nella Modalità Avanzata.

Barra di Attività della Scansione

Puoi usare la barra di scansione per scansionare velocemente files e cartelle (trascinandoli sopra alla barra) Trascinare il file o la cartella che si desidera scansionare sulla barra delle attività di scansione. Seguire le istruzioni della procedura guidata Scansione Antivirus per eseguire la scansione.

Nota

Per ulteriori informazioni, far riferimento a *«Barra di Attività della Scansione»* (p. 27).

32. Programmazione della scansione del computer

Scansionare il computer periodicamente è il modo migliore per assicurare che il computer non abbia malware. Acronis Backup and Security 2010 consente di programmare attività di scansioni di modo che sia possibile scansionare automaticamente il computer.

Per programmare Acronis Backup and Security 2010 affinché scansioni il computer, eseguire i seguenti passi:

1. Aprire Acronis Backup and Security 2010 e passare l'interfaccia utente in Modalità Avanzata.
2. Clicca su **Antivirus** dal menù a sinistra.
3. Fare clic sulla scheda **Scansione Virus**. Qui è possibile trovare un numero di attività di scansione di default ed è possibile creare le proprie attività di scansione.
   - Le attività di sistema sono disponibili e possono essere eseguite da ogni account utente Windows.
   - Le attività dell'utente sono disponibili solo all'utente che le ha create che è l'unico che le può eseguire.

   Queste sono le attività di scansione predefinite che si possono programmare:

Funzione di Default	Descrizione
Scansione del Sistema approfondita	Esamina l'intero sistema. Nella configurazione predefinita, esegue la scansione per tutti i tipi di malware che minacciano la sicurezza del vostro sistema, come virus, spyware, adware, rootkits ed altri.
Scansione sistema	Esamina l'intero sistema, esclusi gli archivi. Nella configurazione di default la scansione ricerca tutti i tipi di malware ad eccezione dei rootkit.
Scansione Veloce del Sistema	Scansiona le cartelle `Windows` e `Program Files`. Nella configurazione predefinita, esamina per cercare tutti i tipi di malware, esclusi i rootkit, ma non esamina la memoria, il registro nè i cookies.
Scansione Autologon	Esamina gli elementi che vengono eseguiti quando un utente accede a Windows. Per utilizzare queste attività, è necessario programmarle per farle eseguire all'avvio del sistema. Di default, la scansione autologon è disabilitata

Funzione di Default	Descrizione
Documenti	Utilizzare questa funzione per esaminare delle cartelle importanti dell'utente corrente: `My Documents`, `Desktop` e `StartUp`. Questo garantirà la sicurezza dei vostri documenti, uno spazio di lavoro sicuro ed applicazioni pulite al avvio.

Se nessuna di queste scansioni soddisfa le proprie esigenze, è possibile creare una nuova attività di scansione, che è poi possibile programmare per l'esecuzione come necessario.

4. Fare clic sulla attività do scansione desiderata e selezionare **Programma**. Apparirà una nuova finestra.
5. Programmare l'attività per l'esecuzione come necessario:
   - Per eseguire l'attività di scansione solo una volta, selezionare **Una volta** e specificare la data e l'ora di avvio.
   - Per eseguire l'attività di scansione dopo l'avvio del sistema, selezionare **All'avvio del sistema**. Specifica dopo quanto tempo dal suo inizio, il compito deve essere fermato.
   - Per eseguire l'attività di scansione regolarmente, selezionare **Periodicamente** e specificare la frequenza, la data e l'ora di avvio.

Nota

Ad esempio, per scansionare il computer ogni sabato alle 2 di notte, è necessario configurare la programmazione nel seguente modo:

a. Selezionare **Periodicamente**.

b. Nel campo **Ogni**, digitare 1 e poi selezionare **settimane** dal menu. In questo modo l'attività viene eseguita una volta alla settimana.

c. Impostare come data di inizio il prossimo sabato.

d. Impostare come ora di inizio `2:00:00`.

6. Fare clic su **OK** per salvare la programmazione. L'attività di scansione verrà eseguita automaticamente in base alla programmazione definita. Se il computer è spento quando deve essere eseguita la programmazione, l'attività verrà eseguita appena si avvia il computer.

Risoluzione dei problemi e aiuto

33. Risoluzione dei problemi

In questo capitolo vengono spiegati alcuni problemi che si possono incontrare utilizzando Acronis Backup and Security 2010 e vengono inoltre fornite possibili soluzioni per questi problemi. La maggior parte di questi problemi possono essere risolti tramite una configurazione appropriata delle impostazioni del prodotto.

Se non è possibile trovare il problema qui, o se la soluzione fornita non lo risolve, è possibile contattare un rappresentante del supporto tecnico di Acronis come delineato nel capitolo «*Supporto*» (p. 320).

33.1. Problemi di installazione

Quest'articolo permette di risolvere i problemi di installazione più comuni di Acronis Backup and Security 2010. Tali problemi possono essere raggruppati nelle seguenti categorie:

- Errori di convalida dell'installazione: non è possibile eseguire l'assistente di setup a causa di condizioni specifiche del sistema.
- Installazione non riuscita: l'installazione è stata avviata dall'assistente di setup ma non è stata completata con successo.

33.1.1. Errori di convalida dell'installazione

Quando viene avviato l'assistente di setup vengono verificate diverse condizioni al fine di convalidare la possibilità di avviare l'installazione. La tabella seguente presenta gli errori di convalida dell'installazione più comuni e le soluzioni per superarli.

Errore	Descrizione e soluzione
Non si dispone di privilegi sufficienti per installare il programma.	Per eseguire l'assistente di setup e installare Acronis Backup and Security 2010 è necessario avere privilegi di amministratore. Eseguire una delle seguenti azioni: ● Accedere ad un account di amministratore di Windows ed eseguire di nuovo l'assistente di setup. ● Fare clic con il pulsante destro sul file di installazione e selezionare **Esegui come**. Digitare il nome utente e la password di un account di amministratore di Windows sul sistema.
Il programma di installazione ha riscontrato una precedente versione di	Acronis Backup and Security 2010 era precedentemente installato sul sistema, ma l'installazione non è stata rimossa completamente.

Errore	Descrizione e soluzione
Acronis Backup and Security 2010 che non è stata disinstallata correttamente.	Questa condizione blocca la nuova installazione di Acronis Backup and Security 2010. Per risolvere questo errore ed installare Acronis Backup and Security 2010, seguire questi passi: 1. Contatti il supporto tecnico Acronis Inc. come descritto nel *«Supporto»* (p. 320) e faccia richiesta per lo strumento di disinstallazione. 2. Eseguire il programma di disinstallazione utilizzando privilegi di amministratore. 3. Riavviare il computer. 4. Avviare di nuovo l'assistente setup per installare Acronis Backup and Security 2010.
Il prodotto Acronis Backup and Security 2010 non è compatibile con il sistema operativo.	Si sta cercando di installare Acronis Backup and Security 2010 su un sistema operativo non supportato. Controllare i *«Requisiti del sistema»* (p. 2) per scoprire su quali sistemi operativi è possibile installare Acronis Backup and Security 2010. Se il sistema operativo è Windows XP con Service Pack 1 o senza alcun service pack, è possibile installare il Service Pack 2 o superiore e quindi eseguire di nuovo l'assistente di setup.
Il file di installazione è progettato per un tipo diverso di processore.	Se viene ricevuto tale errore, significa che si sta tentando di eseguire una versione non corretta del file di installazione. Esistono due versioni del file di installazione di Acronis Backup and Security 2010: una per processori a 32 bit e l'altra per processori a 64 bit. Per assicurarsi di avere la versione corretta per il proprio sistema, scaricare il file di installazione direttamente da http://www.acronis.it/.

33.1.2. Installazione non riuscita

Vi sono diverse possibilità di installazione non riuscita:

- Durante l'installazione appare una schermata di errore. Potrebbe essere richiesto di annullare l'installazione oppure potrebbe esservi un pulsante per avviare lo strumento di disinstallazione in modo da pulire il sistema.

Nota

Immediatamente dopo aver avviato l'installazione si potrebbe ricevere una notifica di spazio libero insufficiente su disco per l'installazione di Acronis Backup and Security 2010. In tal caso liberare lo spazio richiesto sulla partizione dove si desidera installare Acronis Backup and Security 2010 e quindi riprendere o riavviare l'installazione.

- L'installazione si blocca e il sistema potrebbe congelarsi. Solo un riavvio ripristina la capacità di rispondere del sistema.
- L'installazione è stata completata ma è impossibile utilizzare alcune o tutte le funzioni di Acronis Backup and Security 2010.

Per risolvere un'installazione non riuscita ed installare Acronis Backup and Security 2010, seguire questi passi:

1. **Ripulire il sistema dopo l'installazione non riuscita.** Se l'installazione non riesce, alcuni file e alcune chiavi di registro di Acronis Backup and Security 2010 potrebbero rimanere sul sistema. Tali rimanenze potrebbero impedire una nuova installazione di Acronis Backup and Security 2010. Potrebbero inoltre influenzare le prestazioni e la stabilità del sistema. Per questa ragione è necessario rimuoverle prima di tentare nuovamente di installare il prodotto.

   Se la schermata di errore fornisce un pulsante per avviare lo strumento di disinstallazione, fare clic su tale pulsante per ripulire il sistema. Altrimenti procedere nel modo seguente:

   a. Contatti il supporto tecnico Acronis Inc. come descritto nel «*Supporto*» (p. 320) e faccia richiesta per lo strumento di disinstallazione.

   b. Eseguire il programma di disinstallazione utilizzando privilegi di amministratore.

   c. Riavviare il computer.

2. Controllare che non vi siano altri programmi di sicurezza installati che potrebbero interferire con il normale funzionamento di Acronis Backup and Security 2010. Se è così si raccomanda di rimuovere tutti gli altri programmi di sicurezza e quindi installare nuovamente Acronis Backup and Security 2010.

3. Riprovare ad installare Acronis Backup and Security 2010. Si raccomanda di scaricare ed eseguire la versione più recente del file di installazione da www.acronis.it.

4. Se l'installazione non riesce di nuovo, contattare Acronis Inc per avere assistenza come descritto in «*Supporto*» (p. 320).

33.2. I servizi Acronis Backup and Security 2010 non rispondono

Questo articolo aiuta a risolvere i problemi nel caso in cui *I servizi Acronis Backup and Security 2010 non funzionano*. Si potrebbe trovare questo errore:

- L'icona Acronis nell'area di notifica è grigia e un pop-up informa che i servizi Acronis Backup and Security 2010 non rispondono.
- La finestra Acronis Backup and Security 2010 mostra che i servizi Acronis Backup and Security 2010 non stanno rispondendo.

L'errore potrebbe essere causato da una delle seguenti condizioni:

- Si sta installando un aggiornamento importante.
- errori temporanei di comunicazione tra i servizi di Acronis Backup and Security 2010.
- alcuni servizi di Acronis Backup and Security 2010 sono arrestati.
- altri programmi di sicurezza sono in esecuzione sul computer contemporaneamente a Acronis Backup and Security 2010.
- virus presenti nel sistema stanno interferendo con il normale funzionamento di Acronis Backup and Security 2010.

Per risolvere questo errore, provare queste soluzione:

1. Aspettare alcuni momenti e vedere se qualcosa cambia. L'errore potrebbe essere temporaneo.
2. Riavviare il computer e aspettare alcuni attimi fino a quando Acronis Backup and Security 2010 è caricato. Aprire Acronis Backup and Security 2010 per vedere se l'errore persiste. Riavviare il computer di solito risolve il problema.
3. Controllare che non vi siano altri programmi di sicurezza installati che potrebbero interferire con il normale funzionamento di Acronis Backup and Security 2010. Se è così si raccomanda di rimuovere tutti gli altri programmi di sicurezza e quindi installare nuovamente Acronis Backup and Security 2010.
4. Se l'errore persiste, potrebbe essere un problema più serio (ad esempio, ci potrebbe essere un virus che interferisce con Acronis Backup and Security 2010). Rivolgersi a Acronis Inc per supporto come descritto nella sezione *«Supporto»* (p. 320).

33.3. La condivisione file e stampanti sulla Rete Wi-Fi (Wireless) non funziona.

Questo articolo permette di risolvere i seguenti problemi del firewall Acronis Backup and Security 2010 nelle reti Wi-Fi:

- Impossibile condividere i file con i computer sulla rete Wi-Fi.
- Impossibile accedere ad una stampante di rete collegata ad una rete Wi-Fi.
- Impossibile accedere ad una stampante condivisa da un computer sulla rete Wi-Fi.
- Impossibile condividere la propria stampante con i computer sulla rete Wi-Fi.

Prima di iniziare a risolvere tali problemi è necessario comprendere alcuni aspetti della sicurezza e della configurazione del firewall Acronis Backup and Security 2010 con reti Wi-Fi. Dal punto di vista della sicurezza, le reti Wi-Fi rientrano in una delle seguenti categorie:

- **Reti Wi-Fi sicure.** Questo tipo di rete permette la connessione solo di dispositivi Wi-Fi autorizzati. L'accesso alla rete è regolato da una password. Un esempio di reti Wi-Fi sicure è una rete installata in un ufficio.
- **Reti Wi-Fi aperte (non sicure).** Qualsiasi dispositivo Wi-Fi entro il raggio di ricezione di una rete Wi-Fi non sicura può effettuare liberamente la connessione. Le reti Wi-Fi non sicure sono di vasto impiego. Includono praticamente tutte le reti Wi-Fi pubbliche (ad esempio in scuole, internet café, aeroporti e così via). Anche una rete domestica basata su un router wireless non è sicura fino a quando non viene attivata la sicurezza del router.

  Le reti Wi-Fi non sicure presentano un grande rischio per la sicurezza perchè il computer è collegato ad altri computer sconosciuti. Senza l'adeguata protezione fornita da un firewall, chiunque sia collegato alla rete può accedere alle vostre condivisioni e perfino penetrare nel computer.

Quando si è connessi ad una rete Wi-Fi non sicura, Acronis Backup and Security 2010 blocca automaticamente le connessioni con i computer sulla rete. L'accesso a Internet rimane possibile ma non è possibile condividere file o stampanti con altri utenti della rete.

Per abilitare la comunicazione con una rete Wi-Fi, vi sono due soluzioni:

- La soluzione "computer affidabile" permette la condivisione di file e stampanti solo con computer specifici (computer affidabili) sulla rete Wi-Fi. Utilizzare questa soluzione quando si è connessi ad una rete Wi-Fi pubblica (ad esempio a scuola o in un internet café) e si desidera condividere file o stampanti con un amico, oppure si vuole accedere ad una stampante di rete Wi-Fi.
- La soluzione "rete sicura" permette la condivisione di file e stampanti per l'intera rete Wi-Fi (rete sicura). Questa soluzione non è consigliata per motivi di sicurezza, ma può essere utile in determinate situazioni (ad esempio è possibile utilizzarla per una rete Wi-Fi domestica o in ufficio).

33.3.1. Soluzione "Computer Affidabili"

Per configurare il firewall Acronis Backup and Security 2010 in modo da permettere la condivisione di file o stampanti con un computer sulla rete Wi-Fi, o l'accesso ad una stampante di rete Wi-Fi, seguire questi passi:

1. Aprire Acronis Backup and Security 2010 e passare l'interfaccia utente in Modalità Avanzata.
2. Fare clic su **Firewall** nel menu a sinistra.
3. Fare clic sulla scheda **Rete**.
4. Nella tabella Zone, selezionare la rete Wi-Fi e quindi fare clic sul pulsante **Aggiungi**.
5. Selezionare il computer desiderato o la stampante di rete Wi-Fi dall'elenco di dispositivi rilevati sulla rete Wi-Fi. Se tale computer o stampante non è stato rilevato automaticamente, è possibile digitare l'indirizzo IP nel campo **Zona**.
6. Selezionare l'azione **Permetti**.
7. Selezionare **OK**.

Se si continua a non riuscire a condividere i file o la stampante con il computer selezionato, probabilmente la causa non è dovuta al firewall Acronis Backup and Security 2010 sul vostro computer. Controllare altre potenziali cause, ad esempio le seguenti:

- Il firewall dell'altro computer potrebbe bloccare la condivisione di file e stampanti in reti Wi-Fi non sicure (pubbliche).
  - Nel caso in cui il firewall Acronis Backup and Security 2010 sia in uso, è necessario seguire la stessa procedura sull'altro computer per permettere la condivisione di file e stampanti con il proprio computer.
  - Se viene utilizzato il firewall di Windows, è possibile configurarlo per permettere la condivisione di file e stampanti nel modo seguente: aprire la finestra delle impostazioni di Windows Firewall, scheda **Eccezioni** e selezionare la casella di controllo **Condivisione File e Stampanti**.
  - Se viene utilizzato un altro programma firewall, fare riferimento alla sua documentazione o al file della guida.
- Condizioni generiche che possono impedire l'utilizzo o la connessione ad una stampante condivisa:
  - Potrebbe essere necessario accedere ad un account di amministratore di Windows per poter accedere alla stampante condivisa.
  - Potrebbero essere state impostate delle autorizzazioni per la stampante condivisa che permettono l'accesso solo a specifici computer e utenti. Se si sta condividendo la propria stampante, controllare le autorizzazioni impostate per

la stampante per verificare che l'utente dell'altro computer sia autorizzato ad accedere alla stampante. Se si sta provando a collegarsi ad una stampante condivisa, controllare insieme all'utente dell'altro computer di disporre delle autorizzazioni al collegamento alla stampante.

- La stampante collegata al proprio computer o all'altro computer non è condivisa.
- La stampante condivisa non è stata aggiunta al computer.

Nota

Per apprendere come gestire la condivisione di stampanti (condividere una stampante, impostare o rimuovere autorizzazioni per una stampante, collegarsi ad una stampante di rete o ad una stampante condivisa) andare alla Guida in Linea e Supporto Tecnico di Windows (nel menu Start fare clic su **Guida in Linea e Supporto Tecnico**).

Se si continua a non riuscire ad accedere alla stampante di rete Wi-Fi, probabilmente la causa non è dovuta al firewall Acronis Backup and Security 2010 sul vostro computer. L'accesso alla stampante di rete Wi-Fi potrebbe essere ristretto a specifici computer od utenti. Controllare con l'amministratore della rete Wi-Fi se si dispone delle autorizzazioni al collegamento con tale stampante.

Se si ritiene che il problema sia dovuto al firewall Acronis Backup and Security 2010 è possibile contattare Acronis Inc. per avere assistenza come descritto nella sezione «*Supporto*» (p. 320).

33.3.2. Soluzione "Rete Sicura"

Si consiglia di utilizzare questa soluzione solo per reti Wi-Fi domestiche o in ufficio.

Per configurare il firewall Acronis Backup and Security 2010 in modo da permettere la condivisione di file e stampanti con l'intera rete Wi-Fi, seguire questi passi:

1. Aprire Acronis Backup and Security 2010 e passare l'interfaccia utente in Modalità Avanzata.
2. Fare clic su **Firewall** nel menu a sinistra.
3. Fare clic sulla scheda **Rete**.
4. Nella tabella di Configurazione Rete, colonna **Livello di Fiducia**, fare clic sulla freccia ▾ nella cella corrispondente alla rete Wi-Fi.
5. A seconda del livello di sicurezza che si desidera ottenere, scegliere una delle seguenti opzioni:
   - **Non sicuro** - per accedere ai file e alle stampanti condivise sulla rete Wi-Fi, senza permettere l'accesso alle proprie condivisioni.

- **Sicuro** - per permettere la condivisione di file e stampanti in entrambe le direzioni. Questo significa che gli utenti connessi alla rete Wi-Fi possono accedere ai propri file o stampanti condivisi.

Se si continua a non riuscire a condividere i file o la stampante con specifici computer sulla rete Wi-Fi, probabilmente la causa non è dovuta al firewall Acronis Backup and Security 2010 sul vostro computer. Controllare altre potenziali cause, ad esempio le seguenti:

- Il firewall dell'altro computer potrebbe bloccare la condivisione di file e stampanti in reti Wi-Fi non sicure (pubbliche).
  - ▶ Nel caso in cui il firewall Acronis Backup and Security 2010 sia in uso, è necessario seguire la stessa procedura sull'altro computer per permettere la condivisione di file e stampanti con il proprio computer.
  - ▶ Se viene utilizzato il firewall di Windows, è possibile configurarlo per permettere la condivisione di file e stampanti nel modo seguente: aprire la finestra delle impostazioni di Windows Firewall, scheda **Eccezioni** e selezionare la casella di controllo **Condivisione File e Stampanti**.
  - ▶ Se viene utilizzato un altro programma firewall, fare riferimento alla sua documentazione o al file della guida.
- Condizioni generiche che possono impedire l'utilizzo o la connessione ad una stampante condivisa:
  - ▶ Potrebbe essere necessario accedere ad un account di amministratore di Windows per poter accedere alla stampante condivisa.
  - ▶ Potrebbero essere state impostate delle autorizzazioni per la stampante condivisa che permettono l'accesso solo a specifici computer e utenti. Se si sta condividendo la propria stampante, controllare le autorizzazioni impostate per la stampante per verificare che l'utente dell'altro computer sia autorizzato ad accedere alla stampante. Se si sta provando a collegarsi ad una stampante condivisa, controllare insieme all'utente dell'altro computer di disporre delle autorizzazioni al collegamento alla stampante.
  - ▶ La stampante collegata al proprio computer o all'altro computer non è condivisa.
  - ▶ La stampante condivisa non è stata aggiunta al computer.

Nota

Per apprendere come gestire la condivisione di stampanti (condividere una stampante, impostare o rimuovere autorizzazioni per una stampante, collegarsi ad una stampante di rete o ad una stampante condivisa) andare alla Guida in Linea e Supporto Tecnico di Windows (nel menu Start fare clic su **Guida in Linea e Supporto Tecnico**).

Se si continua a non riuscire ad accedere alla stampante di rete Wi-Fi, probabilmente la causa non è dovuta al firewall Acronis Backup and Security 2010 sul vostro computer. L'accesso alla stampante di rete Wi-Fi potrebbe essere ristretto a specifici computer od utenti. Controllare con l'amministratore della rete Wi-Fi se si dispone delle autorizzazioni al collegamento con tale stampante.

Se si ritiene che il problema sia dovuto al firewall Acronis Backup and Security 2010 è possibile contattare Acronis Inc. per avere assistenza come descritto nella sezione «*Supporto*» (p. 320).

33.4. Il filtro Antispam non funziona appropriatamente

Questo articolo permette di risolvere i seguenti problemi delle operazioni di filtro Antispam di Acronis Backup and Security 2010:

- Un numero di messaggi e-mail legittimi sono contrassegnati come `[spam]`.
- Molti messaggi spam non sono contrassegnati come tali dal filtro antispam.
- Il filtro antispam non rileva nessun messaggio spam.

33.4.1. Messaggi Legittimi sono contrassegnati come [spam]

I messaggi legittimi vengono contrassegnati come `[spam]` semplicemente perchè appaiono come tali al filtro antispam di Acronis Backup and Security 2010. Normalmente è possibile risolvere questo problema configurando adeguatamente il filtro Antispam.

Acronis Backup and Security 2010 aggiunge automaticamente i destinatari dei messaggi e-mail inviati alla lista degli Amici. I messaggi e-mail ricevuti dai contatti nell'elenco degli Amici sono considerati legittimi. Non vengono verificati dal filtro antispam e di conseguenza non vengono mai contrassegnati come `[spam]`.

La configurazione automatica dell'elenco Amici non impedisce gli errori di rilevamento che possono accadere in queste situazioni:

- Si ricevono molte e-mail commerciali richieste come risultato della sottoscrizione a vari siti web. In questo caso la soluzione è di aggiungere gli indirizzi e-mail da cui si ricevono tali messaggi e-mail all'elenco degli Amici.
- Una parte significativa delle vostre e-mail legittime proviene da individui a cui non avete mai inviato e-mail in precedenza, ad esempio clienti, potenziali partner d'affari o altri. In questo caso sono richieste altre soluzioni.

Se si sta utilizzando uno dei programmi di posta elettronica con cui Acronis Backup and Security 2010 si integra, provare le soluzioni seguenti:

1. Indica errori di rilevamento. Questo è utilizzato per addestrare il Motore di Apprendimento (Bayesiano) del filtro antispam ed aiuta a prevenire futuri errori di rilevamento. Il Motore di Apprendimento analizza i messaggi indicati e ne

apprende gli schemi. I successivi messaggi e-mail che corrispondono agli stessi schemi non verranno contrassegnati come `[spam]`.

2. Diminuire il livello di protezione antispam. Diminuendo il livello di protezione, il filtro antispam avrà bisogno di maggiori indicazioni di spam per classificare un messaggio e-mail come spam. Utilizzare questa soluzione solo se molti messaggi legittimi (inclusi i messaggi commerciali richiesti) vengono rilevati scorrettamente come spam.
3. Addestra nuovamente il Motore di Apprendimento (Filtro Bayesiano). Utilizzare questa soluzione solo se le soluzioni precedenti non hanno prodotto risultati soddisfacenti.

Nota

Acronis Backup and Security 2010 si integra nella maggior parte delle applicazioni di posta elettronica comunemente utilizzate per mezzo di una barra degli strumenti antispam di facile utilizzo. Per un elenco completo di applicazioni di posta supportate, fare riferimento a *«Software supportato»* (p. 2).

Se si utilizza un'applicazione di posta differente, non è possibile indicare gli errori di rilevamento ed addestrare il Motore di Apprendimento. Per risolvere il problema provare a diminuire il livello di protezione antispam.

Aggiungi i contatti all'Elenco Amici

Se si sta utilizzando un'applicazione di posta supportata si possono facilmente aggiungere i mittenti dei messaggi legittimi all'elenco degli Amici. Attenersi alla seguente procedura:

1. Nell'applicazione di posta selezionare un messaggio e-mail inviato dal mittente che si desidera aggiungere all'elenco degli Amici.
2. Fare clic sul pulsante **Aggiungi Amico** sulla barra degli strumenti antispam di Acronis Backup and Security 2010.
3. Può essere richiesto di accettare gli indirizzi aggiunti all'elenco degli Amici. Selezionare **Non mostrare di nuovo questo messaggio** e fare clic su **OK**.

Si riceveranno sempre email provenienti da questo indirizzo, indipendentemente dal contenuto del messaggio.

Se si utilizza un'applicazione di posta differente, è possibile aggiungere i contatti all'elenco degli Amici dall'interfaccia di Acronis Backup and Security 2010. Attenersi alla seguente procedura:

1. Aprire Acronis Backup and Security 2010 e passare l'interfaccia utente in Modalità Avanzata.
2. Fare clic su **Antispam** nel menu a sinistra.
3. Fare clic sulla scheda **Stato**.

4. Fare clic su **Gestisci Amici**. Apparirà la finestra di configurazione.
5. Digitare l'indirizzo e-mail da cui si desidera sempre ricevere messaggi e-mail e fare clic sul pulsante per aggiungere l'indirizzo all'elenco degli Amici.
6. Selezionare **OK** per salvare le modifiche e chiudere la finestra.

Indica Errori di Rilevamento

Se si sta utilizzando un'applicazione di posta supportata è possibile correggere facilmente il filtro antispam (indicando quali messaggi e-mail non devono essere contrassegnati come `[spam]`). Facendo ciò si migliorerà considerevolmente l'efficienza del filtro antispam. Attenersi alla seguente procedura:

1. Aprire l'applicazione di posta.
2. Andare alla cartella posta indesiderata dove vengono spostati i messaggi spam.
3. Selezionare il messaggio legittimo scorrettamente contrassegnato come `[spam]` da Acronis Backup and Security 2010.
4. Fare clic sul pulsante **Aggiungi Amico** sulla barra degli strumenti antispam di Acronis Backup and Security 2010 per aggiungere il mittente all'elenco degli Amici. Può essere necessario premere **OK** per confermare. Si riceveranno sempre email provenienti da questo indirizzo, indipendentemente dal contenuto del messaggio.
5. Fare clic sul pulsante **Non è Spam** sulla barra degli strumenti antispam di Acronis Backup and Security 2010 (normalmente posizionata nella parte superiore della finestra del client di posta). Questo indica al Motore di Apprendimento che il messaggio selezionato non è spam. Il messaggio e-mail selezionato verrà spostato nella cartella Inbox. I successivi messaggi e-mail che corrispondono agli stessi schemi non verranno più contrassegnati come `[spam]`.

Diminuzione del Livello di Protezione Antispam

Per diminuire il livello di protezione antispam, seguire questi passaggi:

1. Aprire Acronis Backup and Security 2010 e passare l'interfaccia utente in Modalità Avanzata.
2. Fare clic su **Antispam** nel menu a sinistra.
3. Fare clic sulla scheda **Stato**.
4. Spostare il selettore verso il basso lungo la scala.

Si consiglia di diminuire la protezione di un solo livello ed attendere per un tempo sufficiente a valutarne i risultati. Se molti messaggi e-mail continuano ad essere contrassegnati come `[spam]`, è possibile diminuire ulteriormente il livello di protezione. Se si nota che molti messaggi spam non vengono rilevati, non si dovrebbe diminuire il livello di protezione.

Addestra di nuovo il Motore di Apprendimento (Bayesiano)

Prima di addestrare il Motore di Apprendimento (Bayesiano), preparare una cartella contenente solo messaggi SPAM ed una contenente solo messaggi legittimi. Il Motore di Apprendimento le analizzerà e apprenderà le caratteristiche che definiscono lo spam o i messaggi legittimi che vengono normalmente ricevuti. Affinchè l'addestramento sia efficace devono esservi oltre 50 messaggi per ciascuna categoria.

Per ripristinare il database Bayesiano e addestrare di nuovo il Motore di Apprendimento, seguire questi passaggi:

1. Aprire l'applicazione di posta.
2. Dalla barra degli strumenti antispam di Acronis Backup and Security 2010 fare clic sul pulsante **Wizard** per avviare l'assistente di configurazione antispam. Informazioni dettagliate su questo assistente sono disponibili alla sezione *«Assistente per la Configurazione Antispam»* (p. 279).
3. Selezionare **Avanti**.
4. Selezionare **Ignora questo passaggio** e fare clic su **Avanti**.
5. Selezionare **Svuota il database del filtro antispam** e fare clic su **Avanti**.
6. Selezionare la cartella contenente i messaggi legittimi e fare clic su **Avanti**.
7. Selezionare la cartella contenente i messaggi SPAM e fare clic su **Avanti**.
8. Fare clic su **Termina** per avviare il processo di apprendimento.
9. Quando l'addestramento è completato, fare clic su **Chiudi**.

Chiedere Aiuto

Se questa informazione non è stata utile, è possibile contattare Acronis per avere assistenza, come descritto alla sezione *«Supporto»* (p. 320).

33.4.2. Molti Messaggi Spam non vengono rilevati

Se si ricevono molti messaggi spam che non vengono contrassegnati come `[spam]`, è necessario configurare il filtro antispam di Acronis Backup and Security 2010 in modo da migliorarne l'efficienza.

Se si sta utilizzando uno dei programmi di posta elettronica con cui Acronis Backup and Security 2010 si integra, provare le soluzioni seguenti, una alla volta:

1. Indica messaggi spam non rilevati. Questo è utilizzato per addestrare il Motore di Apprendimento (Bayesiano) del filtro antispam e di norma migliora il rilevamento antispam. Il Motore di Apprendimento analizza i messaggi indicati e ne apprende gli schemi. I successivi messaggi e-mail che corrispondono agli stessi schemi verranno contrassegnati come `[spam]`

2. Aggiungi spammer all'elenco Spammer. I messaggi e-mail ricevuti dagli indirizzi nell'elenco Spammer sono contrassegnati automaticamente come `[spam]`.
3. Aumentare il livello di protezione antispam. Aumentando il livello di protezione, il filtro antispam avrà bisogno di minori indicazioni di spam per classificare un messaggio e-mail come spam.
4. Addestra nuovamente il Motore di Apprendimento (Filtro Bayesiano). Utilizzare questa soluzione quando il rilevamento dello spam è molto insoddisfacente e l'indicazione di messaggi spam non rilevati non funziona più.

Nota

Acronis Backup and Security 2010 si integra nella maggior parte delle applicazioni di posta elettronica comunemente utilizzate per mezzo di una barra degli strumenti antispam di facile utilizzo. Per un elenco completo di applicazioni di posta supportate, fare riferimento a *«Software supportato»* (p. 2).

Se si utilizza un'applicazione di posta differente, non è possibile indicare gli errori di rilevamento ed addestrare il Motore di Apprendimento. Per risolvere il problema provare a aumentare il livello di protezione antispam e ad aggiungere gli spammer all'elenco Spammer.

Indica Messaggi Spam non rilevati

Se si utilizza un'applicazione di posta supportata si può facilmente indicare quali messaggi e-mail avrebbero dovuto essere rilevati come spam. Facendo ciò si migliora considerevolmente l'efficienza del filtro antispam. Attenersi alla seguente procedura:

1. Aprire l'applicazione di posta.
2. Andare alla cartella Inbox.
3. Selezionare i messaggi di spam non rilevati.
4. Fare clic sul pulsante **E' Spam** sulla barra degli strumenti antispam di Acronis Backup and Security 2010 (normalmente posizionata nella parte superiore della finestra del client di posta). Questo indica al Motore di Apprendimento che i messaggi selezionati sono spam. Vengono immediatamente contrassegnati come `[spam]` e verranno spostati alla cartella posta indesiderata. I successivi messaggi e-mail che corrispondono agli stessi schemi verranno contrassegnati come `[spam]`

Aggungere Spammer all'Elenco Spammer

Se si sta utilizzando un'applicazione di posta supportata si possono facilmente aggiungere i mittenti dei messaggi di spam all'elenco degli Spammer. Attenersi alla seguente procedura:

1. Aprire l'applicazione di posta.
2. Andare alla cartella posta indesiderata dove vengono spostati i messaggi spam.

3. Selezionare i messaggi contrassegnati come `[spam]` da Acronis Backup and Security 2010.
4. Fare clic sul pulsante **Aggiungi Spammer** sulla barra degli strumenti antispam di Acronis Backup and Security 2010.
5. Può essere richiesto di accettare gli indirizzi aggiunti all'elenco degli Spammer. Selezionare **Non mostrare di nuovo questo messaggio** e fare clic su **OK**.

Se si sta utilizzando un'applicazione di posta differente è possibile aggiungere manualmente gli spammer all'elenco Spammer dall'interfaccia di Acronis Backup and Security 2010. Si tratta di un metodo conveniente solo quando si ricevono diversi messaggi spam dallo stesso indirizzo e-mail. Attenersi alla seguente procedura:

1. Aprire Acronis Backup and Security 2010 e passare l'interfaccia utente in Modalità Avanzata.
2. Fare clic su **Antispam** nel menu a sinistra.
3. Fare clic sulla scheda **Stato**.
4. Fare clic su **Gestisci Spammer** Apparirà la finestra di configurazione.
5. Digitare l'indirizzo e-mail dello spammer e fare clic sul pulsante per aggiungere l'indirizzo all'elenco Spammer.
6. Selezionare **OK** per salvare le modifiche e chiudere la finestra.

Aumento del Livello di Protezione Antispam

Per aumentare il livello di protezione antispam, seguire questi passaggi:

1. Aprire Acronis Backup and Security 2010 e passare l'interfaccia utente in Modalità Avanzata.
2. Fare clic su **Antispam** nel menu a sinistra.
3. Fare clic sulla scheda **Stato**.
4. Spostare il selettore verso l'alto lungo la scala.

Addestra di nuovo il Motore di Apprendimento (Bayesiano)

Prima di addestrare il Motore di Apprendimento (Bayesiano), preparare una cartella contenente solo messaggi SPAM ed una contenente solo messaggi legittimi. Il Motore di Apprendimento le analizzerà e apprenderà le caratteristiche che definiscono lo spam o i messaggi legittimi che vengono normalmente ricevuti. Affinchè l'addestramento sia efficace devono esservi oltre 50 messaggi per ciascuna cartella.

Per ripristinare il database Bayesiano e addestrare di nuovo il Motore di Apprendimento, seguire questi passaggi:

1. Aprire l'applicazione di posta.

2. Dalla barra degli strumenti antispam di Acronis Backup and Security 2010 fare clic sul pulsante **Wizard** per avviare l'assistente di configurazione antispam. Informazioni dettagliate su questo assistente sono disponibili alla sezione *«Assistente per la Configurazione Antispam»* (p. 279).
3. Selezionare **Avanti**.
4. Selezionare **Ignora questo passaggio** e fare clic su **Avanti**.
5. Selezionare **Svuota il database del filtro antispam** e fare clic su **Avanti**.
6. Selezionare la cartella contenente i messaggi legittimi e fare clic su **Avanti**.
7. Selezionare la cartella contenente i messaggi SPAM e fare clic su **Avanti**.
8. Fare clic su **Termina** per avviare il processo di apprendimento.
9. Quando l'addestramento è completato, fare clic su **Chiudi**.

Chiedere Aiuto

Se questa informazione non è stata utile, è possibile contattare Acronis per avere assistenza, come descritto alla sezione *«Supporto»* (p. 320).

33.4.3. Il Filtro Antispam non rileva alcun messaggio spam

Se nessun messaggio spam viene contrassegnato come `[spam]`, potrebbe esserci un problema relativo al filtro Antispam Acronis Backup and Security 2010. Prima di risolvere questo problema, assicurarsi che non sia causato da una delle seguente condizioni:

- La protezione antispam Acronis Backup and Security 2010 è disponibile solo per client e-mail configurati per ricevere messaggi e-mail tramite il protocollo POP3. Questo vuol dire che:
  - ▶ I messaggi e-mail ricevuti tramite servizi e-mail web (ad esempio Yahoo, Gmail, Hotmail o altri) non sono filtrati per spam da Acronis Backup and Security 2010.
  - ▶ Se il proprio client e-mail è configurato per ricevere messaggi e-mail usando un protocollo diverso da POP3 (per esempio, IMAP4), il filtro Antispam Acronis Backup and Security 2010 non verifica se siano spam.

Nota

POP3 è uno dei protocolli più usati per scaricare messaggi e-mail da un server di posta. Se non si conosce il protocollo usato dal proprio client e-mail per scaricare messaggi e-mail, chiedere alla persona che ha configurato il proprio client e-mail.

- Acronis Backup and Security 2010 non esegue la scansione del traffico POP3 di Lotus Notes.

Si dovrebbero inoltre verificare le seguenti possibili cause:

1. Assicurarsi che Antispam sia abilitato.
   a. Apri Acronis Backup and Security 2010.
   b. Fare clic sul pulsante **Impostazioni** in alto a destra.
   c. Nella categoria di impostazioni di sicurezza, verificare lo status antispam.

   Se Antispam è disabilitato, questa è la causa dei problemi. Abilitare Antispam e monitorare il funzionamento dell'antispam per vedere se il problema è risolto.
2. Sebbene non sia molto probabile, si consiglia di verificare se Acronis Backup and Security 2010 è stato configurato per non contrassegnare i messaggi spam come `[spam]`.
   a. Aprire Acronis Backup and Security 2010 e passare l'interfaccia utente in Modalità Avanzata.
   b. Fare clic su **Antispam** sul menu di sinistra e poi sulla scheda **Impostazioni**.
   c. Assicurarsi che l'opzione **Segnare messaggi spam nell'oggetto** sia selezionata.

Una possibile soluzione consiste nel riparare o reinstallare il prodotto. Tuttavia si consiglia di contattare Acronis Inc per supporto, come descritto nella sezione «*Supporto*» (p. 320).

33.5. Rimozione di Acronis Backup and Security 2010 non riuscita

Questo articolo permette di risolvere gli errori che potrebbero verificarsi nella rimozione di Acronis Backup and Security 2010. Vi sono due possibili situazioni:

- Durante la rimozione appare una schermata di errore. La schermata fornisce un pulsante per avviare uno strumento di disinstallazione che pulirà il sistema.
- La rimozione si blocca e il sistema potrebbe congelarsi. Fare clic su **Annulla** per annullare la rimozione. Se questo non dovesse funzionare, riavviare il sistema.

Se la rimozione non riesce, alcuni file e alcune chiavi di registro di Acronis Backup and Security 2010 potrebbero rimanere sul sistema. Tali rimanenze potrebbero impedire una nuova installazione di Acronis Backup and Security 2010. Potrebbero inoltre influenzare le prestazioni e la stabilità del sistema. Per rimuovere completamente Acronis Backup and Security 2010 dal sistema è necessario avviare lo strumento di disinstallazione.

Se la rimozione non riesce con una schermata di errore, fare clic sul pulsante per avviare lo strumento di disinstallazione e ripulire il sistema. Altrimenti procedere nel modo seguente:

1. Contatti il supporto tecnico Acronis Inc. come descritto nel «*Supporto*» (p. 320) e faccia richiesta per lo strumento di disinstallazione.

2. Eseguire il programma di disinstallazione utilizzando privilegi di amministratore. Il tool di disinstallazione rimuoverà tutti i file e chiavi di registro che non siano stati rimossi durante il processo automatico di rimozione.
3. Riavviare il computer.

Se questa informazione non è stata utile, è possibile contattare Acronis per avere assistenza, come descritto alla sezione «*Supporto*» (p. 320).

34. Supporto

Per qualsiasi domanda sui nostri prodotti o per richiedere assistenza, visitare il nostro sito web all'indirizzo http://www.acronis.it.

Glossario

ActiveX

ActiveX è una modalità di scrittura dei Programmi affinché possano essere invocati da altri Programmi e sistemi operativi. La tecnologia ActiveX viene utilizzata con Microsoft Internet Explorer per generare pagine Web interattive che sembrino e si comportino come applicazioni e non come semplici pagine statiche. Con gli elementi ActiveX, gli utenti possono chiedere o rispondere a domande, adoperare dei pulsanti ed interagire in altri modi con la pagina Web. I controlli ActiveX vengono spesso scritti utilizzando il linguaggio Visual Basic.

Gli ActiveX sono noti per una totale mancanza di controlli di sicurezza; gli esperti di sicurezza dei computer scoraggiano il loro utilizzo attraverso Internet.

Adware

L' adware è spesso combinato con un' applicazione Host offerta senza spese quando l'utente accetta l'adware. Le applicazioni adware vengono di solito installate dopo che l'utente ha accettato l'accordo di licenza, dove si spiega il proposito della applicazione. Non viene commesa quindi alcuna offesa o scortesia.

Comunque, i pop-up di avvertimento possono rappresentare un fastidio, ed in alcuni casi degrada il funzionamento del sistema. Inoltre, l'informazione che viene raccolta da queste applicazioni può causare inconvenienti riguardo alla privacy degli utenti non completamente ben informati sui termini del'accordo di licenza.

Archivia

Disco, nastro o cartella che contiene file memorizzati.

Un file che contiene uno o più file in forma compressa.

Backdoor

Breccia nella sicurezza di un programma deliberatamente implementata dal costruttore o dal manutentore. La presenza di tali "brecce" non sempre è dolosa: su alcuni sistemi operativi, ad esempio, vengono utilizzate per l'accesso con utenze privilegiate per servizi tecnici o per i programmatori del venditore a scopo di manutenzione.

Settore di boot

Settore all'inizio di ogni disco che identifica l'architettura del disco (dimensione del settore, dimensione del cluster, ecc.). Nei dischi di avvio, il settore di boot contiene anche un programma che carica il sistema operativo.

Virus di boot

Virus che infetta il settore di boot di un disco rigido oppure di un'unità floppy. Qualsiasi tentativo di effettuare il boot da un disco floppy infetto con un virus di boot, farà sì che il virus venga attivato nella memoria. Da quel momento in

poi, ogni volta che si esegue il boot del sistema, il virus sarà attivo nella memoria.

Browser

Abbreviazione di Web browser, un'applicazione software utilizzata per localizzare e visualizzare pagine Web. I due browser più noti sono Netscape Navigator e Microsoft Internet Explorer. Entrambi sono Browser grafici, ovvero in grado di visualizzare sia grafici che testo. Inoltre, i browser più moderni possono presentare informazioni multimediali, incluso suoni e animazione, nonostante richiedano i plug-in per alcuni formati.

Linea di commando

In un'interfaccia a linea di comando, l'utente digita i comandi nello spazio previsto direttamente sullo schermo, utilizzando il linguaggio di commando.

Cookies

Nell'industria di Internet, i cookie vengono descritti come piccoli file contenenti informazioni relative ai computer individuali che possono essere analizzate e utilizzate dai pubblicitari per tenere traccia dei vostri interessi e gusti online. In questo regno, la tecnologia dei cookie è ancora in fase di sviluppo e l'intenzione è quella di fornire direttamente ciò che si dichiara essere il proprio interesse. Per molte persone è una lama a doppio taglio, poiché da una parte è efficace e consente di far vedere solo ciò che viene dichiarato interessante. Dall'altra parte, implica in effetti un "tracciamento" di dove si va e di cosa si seleziona. Comprensibilmente in questo modo nascerà un dibattito relativo alla riservatezza e molte persone si sentono offese all'idea di essere visti come un " SKU number" (il codice a barre sul retro delle confezioni che vengono passati alla scansione della cassa). Se questo punto di vista può essere considerato estremo, in alcuni casi può essere corretto.

Disk drive

È un dispositivo che legge e scrive dei dati su un disco.

Un drive di disco rigido legge e scrive dischi rigidi.

Un drive di floppy accede i dischi floppy.

I drive di disco possono essere interni (incorporati all'interno di un computer) oppure esterni (collocati in un meccanismo separato e connesso al computer).

Download

Per copiare dati (solitamente un file intero) da un'origine principale su un dispositivo periferico. Il termine viene spesso utilizzato per descrivere un processo di copia di un documento da un servizio on-line sul computer di un utente. Si può inoltre riferire al processo di copiatura di un file da un file server di rete su un computer della rete.

E-mail
Posta elettronica. Servizio che invia messaggi ai computer attraverso reti locali o globali.

Eventi
Azione oppure avvenimento rilevato da un programma. Gli eventi possono rappresentare azioni dell’utente, come fare un clic con il mouse o premere un tasto sulla tastiera oppure avvenimenti del sistema, ad esempio memoria insufficiente.

Falso positivo
Appare quando un prodotto di analisi antivirus individua un documento come infettato quando di fatto non lo è.

Estensione del nome di un file
Porzione del nome di un file che segue il punto finale e che indica il tipo di dati inclusi nel file.

Molti sistemi operativi utilizzano estensioni del nome del file, come Unix, VMS e MS-DOS. Sono normalmente composti da uno a tre lettere (alcuni vecchi supporti OS non più di tre). Esempi: “c” per codici sorgente C, “ps” per PostScipt, “txt” per testi arbitrari.

Euristico
Un metodo basato su regole per l’identificazione di nuovi virus. Questo metodo di scansione non si basa su specifiche impronte dei virus. Il vantaggio della scansione euristica è di non venire ingannata dalle nuove varianti dei virus esistenti. Può comunque occasionalmente segnalare codici sospetti in programmi normali, generando "falsi positivi".

IP
Internet Protocol – protocollo di instradamento nella suite di protocollo TCP/IP, responsabile dell’indirizzamento IP, dell’instradamento, della frammentazione e della ricomposizione dei pacchetti IP.

Applet Java
Programma Java concepito per funzionare solo su pagine web. Per utilizzare un applet su una pagina web, bisognerà specificare il nome dell’applet e la dimensione (lunghezza e larghezza -in pixel) che l’applet può utilizzare. Quando si accede alla pagina web, il browser scarica l’applet dal server e lo esegue sulla macchina dell’utente (il client). Gli Applet differiscono dalle applicazioni in quanto sono governati da un rigido protocollo di sicurezza.

Ad esempio, nonostante gli applet vengano lanciati sul client, essi non possono leggere o scrivere dati nella macchina dell’utente. Inoltre, gli applet sono ulteriormente limitati in modo che possano leggere e scrivere dati solo dallo stesso dominio dai quali provengono.

Macro virus

Tipo di virus del computer codificato come macro all'interno di un documento. Molte applicazioni, come ad esempio Microsoft Word ed Excel, supportano potenti linguaggi macro.

Queste applicazioni consentono di codificare una macro in un documento e di eseguire la macro ogni volta che il documento viene aperto.

Client mail

Un client e-mail è un'applicazione che vi consente di inviare e ricevere e-mail.

Memoria

Aree di immagazzinaggio interne nel computer. Il termine memoria identifica l'immagazzinaggio dati sotto forma di chip; la parola storage viene utilizzata per la memoria su nastri o su dischi. Ogni computer dispone di un certo quantitativo di memoria fisica, solitamente chiamata memoria principale oppure RAM.

Non euristico

Questo metodo di scansione si basa su specifiche impronte di virus. Il vantaggio della scansione non-euristica è di non essere ingannato da ciò che potrebbe sembrare un virus e non genera falsi allarmi.

Programmi impaccati

File in formato compresso. Molti sistemi operativi e molte applicazioni contengono comandi che vi consentono di impaccare un file in modo da occupare meno memoria. Ad esempio, supponiamo che abbiate un file di testo che contenga dieci caratteri spazio consecutivi. Normalmente occuperebbe dieci byte di memoria.

Un programma che impacca i file sostituirebbe gli spazi con un carattere speciale serie_di_spazi seguito dal numero di spazi sostituiti. In questo caso i dieci spazi occuperebbero solo due byte. Questa è solo una tecnica di impaccaggio – ce ne sono molte altre.

Percorso

Le esatte direzioni per raggiungere un file su un computer. Queste direzioni vengono solitamente descritte attraverso il sistema di casellario gerarchico dall'alto al basso.

La strada tra due punti qualsiasi, come ad esempio il canale di comunicazioni tra due computer.

Phishing

L'atto d'inviare una mail ad un utente fingendo di essere una ditta legittima ed affermata, nel tentativo di truffare l'utente, facendole cedere informazione privata che verrà usata per furti d'identità. La e-mail indirizza gli utenti a visitare una pagina Web, dove gli viene chiesto di aggiornare informazioni personali, come password e carte di credito, numero della previdenza sociale e del conto

in banca, che questa legittima organizzazione ha già. In ogni caso, la pagina Web è finta, e organizzata soltanto per rubare l'informazione del utente.

Virus polimorfico

Virus che modifica la propria forma con ogni file che infetta. In quanto non dispongono di caratteristiche binarie costanti, tali virus sono difficili da identificare.

Porta

Interfaccia su un computer alla quale è possibile connettere un supporto. I Personal Computer hanno vari tipi di porte. Internamente ci sono varie porte per la connessione di unità disco, schermi e tastiere. Esternamente i Personal Computer hanno porte per la connessione dei modem, delle stampanti, dei mouse e altri supporti periferici.

Nelle reti TCP/IP e UDP, un punto di arrivo ad una connessione logica. Il numero della porta identifica di che tipo di porta si tratta. Ad esempio, la porta 80 viene usata per il traffico HTTP.

File di report

File che elenca le azioni avvenute. Acronis Backup and Security 2010 mantiene un file di rapporto che elenca i percorsi esaminati, le cartelle, il numero di archivi e file esaminati, quanti file infetti e sospetti sono stati trovati.

Rootkit

Un rootkit è una serie di strumenti software che offre accesso a livello di amministratore ad un sistema. Il termine fu usato per la prima volta per i sistemi operativi UNIX e faceva riferimento a strumenti ricompilati che fornivano agli intrusi i diritti di amministratore, consentendo loro di celare la loro presenza in modo da non dover essere visti dagli amministratori del sistema.

Il ruolo principale dei rootkit è nascondere i processi, i file, i login e i log. Possono anche intercettare dati dai terminali, dalle connessioni di rete o dalle periferiche, se incorporano il software adeguato.

I rootkit non sono maligni per natura. Ad esempio, i sistemi e persino alcune applicazioni nascondono file critici utilizzando rootkit. Comunque, essi vengono principalmente utilizzati per nascondere malware o per celare la presenza di un intruso nel sistema. Se combinati al malware, i rootkit rappresentano una grave minaccia per l'integrità e la sicurezza di un sistema. Possono monitorare il traffico, creare backdoor nel sistema, alterare file e log ed evitare il rilevamento.

Script

Altro termine per macro o file batch, uno script è una lista di comandi che possono essere eseguiti senza interazione con l'utente.

Spam

Posta elettronica pubblicitaria. Generalmente conosciuto come qualsiasi e-mail non richiesta.

Spyware

Accede alla connessione internet dell'utente senza che l'utente se ne accorga, normalmente a scopo pubblicitario. Le applicazioni Spyware vengono tipicamente come un componente nascosto di programmi freeware o shareware che possono essere scaricati da Internet. Tuttavia, deve essere segnalato che la maggioranza delle applicazioni shareware o freeware non arrivano con spyware. Una volta installato, lo spyware esegue il monitoraggio dell'attività dell' utente su Internet e trasmette questa informazione di nascosto a qualcun altro. Lo spyware può anche raccogliere informazione su indirizzi mail e addirittura passwords e numeri di carta di credito.

Lo spyware è simile a un Cavallo di Troia che gli utenti installano senza volere quando installano qualcos'altro. Un modo comune di diventare una vittima dello spyware è scaricare certi file peer-to-peer scambiando prodotti che sono disponibili oggi.

A parte delle questioni dell'etica e la privacy, lo spyware approfitta dell' utente usando risorse di memoria del computer "mangiandosi" larghezza di banda dal momento in cui invia informazione alla sua "casa" usando l' internet dell' utente. Dato che lo spyware sta usando memoria e risorse del sistema, le applicazioni eseguite in sottofondo (background) possono portare alla caduta del sistema o alla instabilità.

Elementi di startup

Qualsiasi file posizionato in questa cartella si aprirà quando il computer viene avviato. Ad esempio, una schermata di avvio, un file sonoro da eseguire quando il computer si avvia la prima volta, una agenda-calendario, oppure programmi applicativi che possono essere elementi di startup. Normalmente in questa cartella viene posizionato un alias di un file, anziché il file stesso.

Barra di sistema

Introdotta con Windows 95, la barra delle applicazioni è situata nella barra degli strumenti di Windows (solitamente in basso vicino all'orologio) e contiene icone miniaturizzate per un semplice accesso alle funzioni di sistema, ad esempio il fax, la stampante, il modem, il volume ed altro. Fare doppio clic o fare clic con il pulsante destro su un'icona per vedere ed accedere ai dettagli e ai controlli.

TCP/IP

Transmission Control Protocol/Internet Protocol – Insieme di protocolli di networking largamente utilizzati su Internet che consentono le comunicazioni attraverso le reti interconnesse di computer con diverse architetture hardware e vari sistemi operativi. TCP/IP include gli standard su come comunicano i computer e le convenzioni per connettere le reti e il traffico di instradamento.

Trojan

Programma distruttivo che si maschera da applicazione benevola. Diversamente dai virus, i cavalli di Troia non si replicano ma possono comunque essere altrettanto distruttivi. Un tipo di cavallo di Troia particolarmente insidioso è un programma che dichiara di pulire i virus del vostro computer ma che al contrario introduce i virus nel vostro computer.

Il termine deriva dalla storia dell'Iliade di Omero, dove i Greci mandarono un gigantesco cavallo di legno ai loro avversari, i Troiani, apparentemente come offerta di pace. Ma dopo che i Troiani portarono il cavallo all'interno delle mura della loro città, i soldati Greci uscirono dal ventre cavo del cavallo e aprirono le porte della città, consentendo ai loro compatrioti di entrare e catturare Troia.

Aggiorna

La nuova versione di un prodotto software o hardware creato per sostituire una versione precedente dello stesso prodotto. In aggiunta, le routine di installazione degli aggiornamenti spesso verificano e si assicurano che sia già installata una versione precedente sul vostro computer; diversamente non sarà possibile installare l'aggiornamento.

Acronis Backup and Security 2010 dispone del proprio modulo di aggiornamento che consente la verifica manuale degli aggiornamenti oppure l'aggiornamento automatico del prodotto.

Virus

Programma o parte di codice caricato sul vostro computer senza che voi lo sappiate e che viene eseguito contro la vostra volontà. La maggior parte dei virus è anche in grado di auto replicarsi. Tutti i virus del computer sono creati dall'uomo. E' relativamente facile produrre un semplice virus in grado di copiare sé stesso innumerevoli volte. Persino un virus così semplice è pericoloso in quanto utilizzerà velocemente tutta la memoria disponibile e porterà il sistema allo stallo. Un tipo di virus ancora più pericoloso è quello in grado di trasmettere sé stesso attraverso le reti superando i sistemi di sicurezza.

Definizione di virus

Caratteristica binaria di un virus, utilizzata dal programma antivirus alfine di rilevare ed eliminare il virus stesso.

Worm(baco)

Programma che si propaga in una rete, riproducendosi durante lo spostamento. Non si può attaccare ad altri programmi.